RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

IRSN
INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

ELEMENTS OF NUCLEAR SAFETY
PRESSURIZED WATER REACTORS

Jean Couturier, Coordinator

Science and Technology Series

Elements of Nuclear Safety, Radiation Protection and Security Series

edp sciences

Elements of nuclear safety – Pressurized water reactors

Jean Couturier
Coordinator and Senior Editor

edp sciences

The Institute for Radiological Protection and Nuclear Safety (IRSN) is a public body undertaking research and consultancy activities in the field of nuclear safety and radiation protection. It provides public authorities with technical support. It also carries out various public service missions entrusted to it under national regulations. In particular, these include radiological monitoring of the environment and workers in France, managing emergency situations, and keeping the public informed. IRSN makes its expertise available to partners and customers both in France and worldwide.

Printed in France
ISBN (papier): 978-2-7598-2722-0
ISBN (ebook): 978-2-7598-2723-7
ISBN (epub): 978-2-7598-2724-4

DOI: 10.1051/978-2-7598-2722-0

Preface

In IRSN's Science and Technology Series, the new series, Elements of Nuclear Safety, Radiological Protection and Security, like the 1996 publication *Elements of Nuclear Safety* by Jacques Libmann, aims to provide all those whose work involves ionizing radiation, primarily in the nuclear industry, with insight on the technical culture that guides the prevention and management of nuclear safety risks. This new series seeks not only to update the 1996 publication, but also to extend its scope to areas previously covered only slightly or not at all.

In its collection of scientific publications, IRSN promotes the most advanced knowledge acquired either within the Institute or in the context of national or international collaboration, focusing particularly on the educational value of their presentation. With this in mind, the new series sets out to provide clear explanations describing how techniques, ideas, approaches, organizations and regulations have developed over time, along with the questions raised and lessons learned from accidents and operating feedback in general.

For those interested in these issues, the series also aims to provide access to firmly established and proven technical knowledge and information in the corresponding subject areas, in keeping with IRSN's three core values, Knowledge, Independence and Accessibility, as defined in its Code of Ethics and Professional Conduct.

We hope that the Elements of Nuclear Safety, Radiological Protection and Security series, initiated by Jean Couturier, will contribute to disseminating knowledge, especially as the next generation of nuclear scientists and technicians enters the profession.

*
*   *

After the first two books in the series, *Elements of Security and Non-Proliferation* (2017) by Jean Jalouneix and *Elements of Nuclear Safety – Research Reactors* (2019) by Jean Couturier, Hassan Abou Yéhia et al., this book updates and develops certain subjects found in Jacques Libmann's *Elements of Nuclear Safety* (1996), focused mainly on the safety of pressurized water reactors, especially those in the French nuclear power plant fleet.

The first pressurized water reactors implemented in the French nuclear power plant fleet were based on American plants built in the late 1960s and early 1970s. At that time, the world had very limited experience in building facilities of this type. Of course, approaches, analysis methods and safety criteria have evolved since then. The knowledge acquired through research and development, as well as the lessons learned from the world's three most significant nuclear accidents, Three Mile Island in 1979, Chernobyl in 1986 and Fukushima Daiichi in 2011, have largely contributed to these developments. Still more has been learned from operating experience from certain events which, although they were kept under control and did not have serious consequences for people and the environment, were considered sufficiently important in terms of safety to require introducing measures to improve accident prevention and mitigation, as in the case of the partial flooding of the Blayais nuclear power plant site in the Gironde region during the storm that hit France in late December 1999.

In France, these changes are applied to reactors either directly following events, occurring in France or other countries, that are considered as having a significant impact on safety, or during periodic reviews (held every ten years), a practice adopted in France in the 1980s.

Instead of offering a snapshot of the nuclear safety approaches and analytical methods currently applied to these facilities, which have benefited from various changes, a more historical approach has been chosen to provide a better understanding of these developments. The choice of a historical approach also partially determined the arrangement of certain chapters.

The first part of the book presents relatively general fundamental information and concepts that are not specific to pressurized water reactors: the effects of ionizing radiation and the radiological protection system, the organizations involved in nuclear safety in France and their roles, the evolution of regulations, the increasing role of civil society and the international context – two areas that have undergone particularly significant development since the 1990s – and the importance of human and organizational factors for achieving a high level of reliability in nuclear facilities and their operations, which represent complex sociotechnical systems, especially with regard to nuclear power reactors.

Subsequent sections, covering design, operation, lessons learned from the three major accidents mentioned above, and emergency preparedness and response, are much more focused on pressurized water reactors, primarily those in the French nuclear power plant fleet, as well as the same type of reactors operated in other countries which have experienced anomalies or events that have provided beneficial operating feedback for the French nuclear power plant fleet.

Finally, information concerning the contributions of research and development in nuclear safety, as well as simulation software, are included in the last part of the book.

This book demonstrates France's determination to constantly seek improvement in the field of nuclear safety. The historical approach chosen here shows how improvement comes about through questioning and pragmatism. Change is reaching beyond the purely national scene, moving towards European, and even worldwide harmonization of safety-related practices to achieve significant improvements in safety. Such is the challenge of the 'new generation' European Pressurized water Reactor (EPR) developed by French and German power utilities in conjunction with manufacturers in both countries, and commissioning of the Unit 3 at the Flamanville nuclear power plant in France, along with new concepts developed to address certain safety issues, leading to more innovative technical solutions. The need to include core-melt situations in the design requirements for new reactors was one of the major milestones set to achieve an overall improvement in nuclear power reactor safety – adopted in the 1990s in the strategic options taken by France and Germany for the EPR.

After the accident at the Chernobyl nuclear power plant in 1986, an international organization (the International Nuclear Safety Advisory Group) introduced the concept of 'safety culture'; may this book contribute to its advancement.

I would particularly like to thank Jean Couturier, coordinator and senior editor, as well as the many specialists who made valuable contributions to this important compendium, which took almost seven years to prepare and finalize.

Jean-Christophe Niel
IRSN Director General

Foreword

This publication on pressurized water reactors, with a particular focus on the specific characteristics and aspects of nuclear safety and radiological protection, was written essentially by experts of the French Institute for Radiological Protection and Nuclear Safety (IRSN).

Jean Couturier was responsible for the general design and coordination of the project. He contributed significantly to writing the book, including entire chapters, while ensuring harmonization and overall consistency. For many topics, parts of Jacques Libmann's book published in 1996 have been included as such for their historical and educational value.

Daniel Quéniart closely reviewed chapters in their draft version at various stages as the book advanced, providing valuable insight and advice – particularly on issues relevant to the history of nuclear safety.

Emmanuel Wattelle supported coordination of the book's draft version for IRSN's Nuclear Safety Division and contributed to editing and finalizing certain chapters. Stéphanie Graff provided support for finalizing the parts of the book on fuel and accident studies.

Contributors are quoted in full on pages XXXVII-XLII, chapter by chapter.

Marc Vincke and Pieter de Gelder of Bel V, the Belgian technical safety organization, wrote the section on lessons learned in Belgium from the Fukushima Daiichi nuclear power plant accident.

The relatively brief sections on pressure equipment regulations relevant to the nuclear field have taken into account sound advice and insight from the French Nuclear Safety Authority (ASN), in particular from Simon Liu of the Nuclear Pressure

Equipment Department (ASN/DEP) and Rémy Catteau of the Nuclear Power Plant Department (ASN/DPN).

Bertrand de Buchère de l'Épinois and Michel Nédélec, members of the Advisory Committee for Reactors (GPR), contributed respectively to the sections on the World Association of Nuclear Operators (WANO) and the concepts of conservatism and safety margins.

This book assumes that readers have prior knowledge of the basic aspects of pressurized water reactor operation[1]; nevertheless, certain notions have been reviewed, particularly with regard to reactor core physics.

Special attention has been given to acknowledging external sources of information, including illustrations. In this respect, special mention is given to Électricité de France (EDF) for works such as *Mémento sûreté nucléaire en exploitation* (2016) and Jean-Pierre Hutin, *La maintenance des centrales nucléaires* (2016); monographs from the Nuclear Energy Directorate of the French Alternative Energies and Atomic Energy Commission (CEA); official French texts (including regulations); documents available on the websites of Framatome and Orano; publications from the International Atomic Energy Agency (IAEA) and the Nuclear Energy Agency of the Organisation for Economic Co-operation and Development (OECD/NEA), papers delivered at conferences and many others.

Odile Lefèvre contributed to book's reviewing and prepared the work for publication and Georges Goué performed illustrations.

Translation into English was provided by Provence Traduction, with special thanks to Deborah Wirick.

[1] The reader may consult, for example, *La chaudière des réacteurs à eau sous pression* (PWR Nuclear Steam Supply Systems), by P. Coppolani, N. Hassenboehler, J. Joseph, J.-F. Petetrot, J.-P. Py, J.-S. Zampa, INSTN/EDP Sciences, 2004; the book *Physique, fonctionnement et sûreté des REP – Maîtrise des situations accidentelles du système réacteur* (Physics, Operation and Safety of PWRs – Controlling Reactor System Accident Situations), by B. Tarride, INSTN/EDP Sciences, *Collection Génie atomique*, 2013; or Chapter 2, Design and Operation of a Pressurized Water Reactor in the book Nuclear Power Reactor Core Melt Accidents. Current State of Knowledge by D. Jacquemain et al. in IRSN's Science and Technology Series, IRSN/EDP Sciences, 2013.

Contents

Part 1

General Background

Chapter 1

Biological and Health Effects of Ionizing Radiation – The Radiological Protection System

Chapter 2

Organization of Nuclear Safety Control and Regulation for Nuclear Facilities and Activities in France

Chapter 3

The International Dimension and the Social Dimension

Chapter 4

Nuclear Reactors: Complex Sociotechnical Systems – the Importance of Human and Organizational Factors

*

*   *

Part 2
Safety by Design

Chapter 5
The Development of Nuclear Power Using Uranium-235 Fission – A Few Notions of Physics Used in Pressurized Water Reactors

Chapter 6
General Objectives, Principles and Basic Concepts of the Safety Approach

Chapter 7
Safety Options and Considerations at the Design Phase

Chapter 8
Study of Operating Conditions in the Deterministic Safety Analysis

Chapter 9
Loss-of-Coolant Accident

Chapter 10
A Special Issue: Steam Generator Tubes

Chapter 11
Providing for Hazards: General Considerations and Internal Hazards

Chapter 12
Providing for External Hazards

Chapter 13
Complementary Domain of Events

Chapter 14
Development and Use of Probabilistic Safety Assessments

Chapter 15

Aspects Specific to PWR Spent Fuel Storage Pools

Chapter 16
Taking into Account Human and Organizational Factors in Facility Design

Chapter 17

Studying Core-Melt Accidents to Enhance Safety

Chapter 18

New-Generation Reactors

*

* *

Part 3
Safety in Operation

Chapter 19
Startup Tests for Pressurized Water Reactors

Chapter 20
General Operating Rules

Chapter 21
Operating Experience Feedback from Events: Rules and Practices

Chapter 22
Operating Experience from Events Attributable to Shortcomings in Initial Reactor Design or the Quality of Maintenance

Chapter 23
Operating Experience from Events Related to Maintenance Operations, Electrical Power Sources and Distribution, Internal and External Hazards

Chapter 24
Enhanced Protection of Estuary and River Sites: Flooding at the Blayais Nuclear Power Plant and Obstruction of a Water Intake at the Cruas-Meysse Nuclear Power Plant

Chapter 25
Taking into Account Human and Organizational Factors in Facility Operation

Chapter 26
Facility Maintenance

Chapter 27

In-service Monitoring and Inspection of Equipment

Chapter 28

Fuel Management, Monitoring and Developments

Chapter 29

Facility Compliance

Chapter 30
Periodic Reviews

Chapter 31

Optimizing Radiation Protection and Limiting Doses Received by Workers During Operations in a Nuclear Power Plant

*

* *

Part 4
The Accidents at Three Mile Island, Chernobyl and Fukushima Daiichi Nuclear Power Plants, Lessons Learned and Emergency Response Management

Chapter 32
The Three Mile Island Nuclear Power Plant Accident

Chapter 33
Incident and Accident Operation: from the Event-Oriented Approach to the State-Oriented Approach

Chapter 34

The Chernobyl Nuclear Power Plant Accident

Chapter 35

Options and Control of Reactivity Insertion in Pressurized Water Reactors

Chapter 36

The Reactor Accident at the Fukushima Daiichi Nuclear Power Plant and Lessons Learned in France

Chapter 37

Lessons Learned from the Fukushima Daiichi Nuclear Power Plant Accident: Work Conducted by the IAEA and WENRA, Action Taken in Countries Other than France

Chapter 38
Emergency Preparedness and Response

*

* *

Part 5
PWR Safety Studies, R&D and Simulation Software

Chapter 39
PWR Safety Studies and R&D

Chapter 40
Examples of Simulation Software Developed for Safety Analysis of Pressurized Water Reactors

Editors, Contributors and Reviewers

Introduction

J. Couturier

Chapter 1. Biological and Health Effects of Ionizing Radiation – the Radiological Protection System

Written by: Jean-François Lecomte and Jacques Libmann

Contributors and reviewers: Éric Blanchardon and Jean Couturier

Chapter 2. Organization of Nuclear Safety Control and Regulation for Nuclear Facilities and Activities in France

Written by: Stanislas Massieux, Jean Couturier, David Boirel and Véronique Leroyer

Contributors and reviewers: Daniel Quéniart, Simon Liu and Remy Catteau from ASN, Thierry Payen

Chapter 3. The International Dimension and the Social Dimension

Written by: Jean Couturier, Bertrand de Buchère de l'Épinois, Didier Wattrelos, Emmanuel Wattelle, Philippe Volant and Véronique Leroyer

Contributors and reviewers: Joel Bardelay (†), Jean-Luc Chambon, Guy Damette and Jean-Michel Évrard

Chapter 4. Nuclear Reactors: Complex Sociotechnical Systems – the Importance of Human and Organizational Factors

Written by: Jean Couturier and Daniel Tasset

Contributors and reviewers: Nicolas Dechy and Brigitte Le Guilcher

Chapter 5. The Development of Nuclear Power Using Uranium-235 Fission – A Few Notions of Physics Used in Pressurized Water Reactors

Written by: Jean Couturier

Contributors and reviewers: Benoit Normand, Antoine Sanchez, Cédric Laville, Stéphanie Graff, Franck Boreicha, Olivier Marchand, Antonio Sargeni, Gianni Bruna, Aude Taisne and Yves Abou Rjeily

Chapter 6. General Objectives, Principles and Basic Concepts of the Safety Approach

Written by: Jean Couturier, Emmanuel Wattelle and Michel Nédélec

Contributor and reviewer: Sebastian Israel

Chapter 7. Safety Options and Considerations at the Design Phase

Written by: Jean Couturier, Céline Picot, Érik Leclerc, Marc Bouscasse and Jean Gassino

Contributors and reviewers: Caroline Lavarenne, Emmanuel Wattelle and Sébastien Israel

Chapter 8. Study of Operating Conditions in the Deterministic Safety Analysis

Written by: Jean Couturier

Contributors and reviewers: Emmanuel Wattelle and Olivier Dubois

Chapter 9. Loss-of-Coolant Accident

Written by: Sandrine Boutin, Stéphanie Graff and Audrey Bordier

Contributors and reviewers: Christophe Rabe, *Jean Couturier, Daniel Monhardt, Caroline Heib and Frank Dubois*

Chapter 10. A Special Issue: Steam Generator Tubes

Written by: Fabien Fiardet, Gérard Génot and Jean-Pierre Ducasse

Contributors and reviewers: Frédéric Fouquet, Jean Couturier, Stéphanie Graff, Frank Dubois and Cécile Deust d'Haultefoeuille

Chapter 11. Providing for Hazards: General Considerations and Internal Hazards

Written by: Jean Couturier, Marc Bouscasse, Jocelyne Lacoue, Marc Henrio and Pauline Trill-Basillais

Contributors and reviewers: Caroline Lavarenne, Céline Picot, Laurent Gilloteau, Thierry Vinot and Jean Battiston

Chapter 12. Providing for External Hazards

Written by: Jean Couturier, Céline Picot, Érik Leclerc, Jocelyne Lacoue, Julien Espargillière

Contributors and reviewers: Caroline Lavarenne, Christophe Clément, Claire-Marie Duluc, Vincent Rebour, Jacques Ducau, Thierry Vinot and Jean Battiston

Chapter 13. Complementary Domain of Events

Written by: Emmanuel Wattelle and François Corenwinder

Contributors and reviewers: Jean Couturier and Sylvie Lombard

Chapter 14. Development and Use of Probabilistic Safety Assessments

Written by: Frédérique Pichereau, François Corenwinder and Emmanuel Raimond

Chapter 15. Aspects Specific to PWR Spent Fuel Storage Pools

Written by: Laurent Gilloteau

Contributor: Jean Couturier

Chapter 16. Taking into Account Human and Organizational Factors in Facility Design

Written by: Daniel Tasset and Brigitte Le Guilcher

Contributors and reviewers: Nicolas Dechy and Karine Herviou

Chapter 17. Studying Core-Melt Accidents to Enhance Safety

Written by: Didier Jacquemain and Jean Couturier

Contributors and reviewers: Jean-Yves Maguer and Ahmed Bentaib

Chapter 18. New-Generation Reactors

Written by: Yann Flauw and Jean Couturier

Contributors and reviewers: Sébastien Israel and Jean-Marie Mattei

Chapter 19. Startup Tests for Pressurized Water Reactors

Written by: Martial Jorel and Jean Couturier

Contributors and reviewers: Nadia Maaroufi, Pierre Marbach, Jean-Charles Valéro and Patrice Négri

Chapter 20. General Operating Rules

Written by: Fabienne Rousseaux, Jean-Yves Maguer Yves Le Rest and Jean Couurier

Contributors and reviewers: Laurent Gilloteau, Mioara Georgescu, Olivier Dubois, Sébastien Israel and Marie Zamarreno

Chapter 21. Operating Experience Feedback from Events: Roles and Practices

Written by: Jean-Marie Rousseau and Jean Couturier

Contributors and reviewers: Martial Jorel, Emmanuel Wattelle, Hervé Bodineau, Vincent Crutel and Naoelle Matahri

Chapter 22. Operating Experience from Events Attributable to Shortcomings in Initial Reactor Design or the Quality of Maintenance

Written by: Jacques Libmann and Jean Couturier

Contributors: François Corenwinder and Martial Jorel

Chapter 23. Operating Experience from Events Related to Maintenance Operations, Electrical Power Sources and Distribution, Internal and External Hazards

Written by: Vincent Crutel

Contributors and reviewers: Jean Couturier and Martial Jorel

Chapter 24. Enhanced Protection of Estuary and River Sites: Flooding at the Blayais Nuclear Power Plant and Obstruction of a Water Intake at the Cruas-Meysse Nuclear Power Plant

Written by: Vincent Crutel and Jean Couturier

Reviewer: Martial Jorel

Chapter 25. Taking into Account Human and Organizational Factors in Facility Operation

Written by: Nicolas Dechy

Contributors and reviewers: Valérie Vassent, Olivier Chanton, Joël Garron and Daniel Tasset

Chapter 26. Facility Maintenance

Written by: Naoelle Matahri

Contributors and reviewers: Jean Couturier, Olivier Elsensohn, Mikael Achour, Martial Jorel and Emmanuel Wattelle

Chapter 27. In-service Monitoring and Inspection of Equipment

Written by: Jean Couturier

Reviewers: Thierry Payen, Bernard Monnot, Thierry Sollier, Olivier Loiseau, François Tarallo, Lili Ducousso Ganjehi and Christine Delaval

Chapter 28. Fuel Management, Monitoring and Developments

Written by: Jean Couturier, Stéphanie Graff and Nicolas Sendecki

Contributors and reviewers: Sandrine Boutin, Olivier Marchand, Cécile Debaudringhien and Aude Taisne

Chapter 29. Facility Compliance

Written by: Anne Tenaud

Contributors and reviewers: Laurent Gilloteau and Olivier Elsensohn

Chapter 30. Periodic Reviews

Written by: Christian Pignolet and Jean Couturier

Contributors and reviewers: Laurent Gilloteau, Marie Zamarreno, François Corenwinder, Pierre Faillard and Naoelle Matahri

Chapter 31. Optimizing Radiation Protection and Limiting Doses Received by Workers During Operations in a Nuclear Power Plant

Written by: Jean Couturier

Contributors and reviewers: Olivier Couasnon, Patrick Jolivet and Philippe Dubiau

Chapter 32. The Three Mile Island Nuclear Power Plant Accident

Written by: Didier Jacquemain and Jean Couturier

Contributors and reviewers: Karine Herviou, Jean-Luc Stephan, Jean-Pierre Ducasse and Nicolas Dechy

Chapter 33. Incident and Accident Operation: from the Event-Oriented Approach to the State-Oriented Approach

Written by: Yves Le Reste and Jean Couturier

Chapter 34. The Chernobyl Nuclear Power Plant Accident

Written by: Jacques Libmann and Jean Couturier

Contributors and reviewers: Philippe Renaud and Dominique Laurier

Chapter 35. Options and Control of Reactivity Insertion in Pressurized Water Reactors

Written by: Delphine Plassard, Jean Couturier, Antoine Sanchez, Caroline Heib and Caroline Lavarenne

Contributors and reviewers: Olivier Marchand, Yves Abou Rjeily, Aude Taisne and Franck Dubois

Chapter 36. The Reactor Accident at the Fukushima Daiichi Nuclear Power Plant and Lessons Learned in France

Written by: Jean Couturier, Emmanuel Wattelle and Philippe Renaud

Contributor: Hervé Bodineau

Chapter 37. Lessons Learned from the Fukushima Daiichi Nuclear Power Plant Accident: Work Conducted by the IAEA and WENRA, Action Taken in Countries Other than France

Written by: Jean Couturier, as well as Marc Vincke and Pieter De Gelder from Bel V

Chapter 38. Emergency Preparedness and Response

Written by: Joel Bardelay (†), Éric Vial and Jean Couturier

Contributors and reviewers: Alain Rannou, Philippe Dubiau, Sylvie Supervil, Jean-Michel Deligne, Cyril Huet and Éric Cogez

Chapter 39. PWR Safety Studies and R&D

Written by: Jean Couturier and Michel Schwarz

Contributors and reviewers: Jean-Michel Évrard, Didier Jacquemain and Thierry Albiol

Chapter 40. Examples of Simulation Software Developed for Safety Analysis of Pressurized Water Reactors

Written by: Jean Couturier, Antonio Sargeni, Caroline Heib, Jocelyne Lacoue and Laurent Audoin

Contributors and reviewers: Gianni Bruna, Ludovic Maas and Didier Jacquemain

Introduction

Nuclear facilities carry specific risks since, by definition, they all contain more or less significant amounts of radioactive substances. These substances may cause workers or the public to be exposed to ionizing radiation and its effects and could have a radiological impact on the environment. Nuclear facilities that generate electrical power naturally come under this category.

Other energy sources also present risks, but the purpose of this book is not to make comparisons. The focus will be limited to presenting the objectives, concepts and principles used to achieve a satisfactory level of safety in nuclear power reactors, and explaining how they are applied when designing and operating these reactors.

Safety is the result of a set of technical and organizational measures taken at all stages in the 'lifetime' of a facility to ensure that its operation and its very existence present risks that are low enough to be considered acceptable for the workers and staff directly involved, the general public and the environment. The concept of 'acceptable risk' does not refer to defined and absolute criteria. It is the result of socio-political choices that evolve over time and may differ from one country to another depending on the local economic situation. While the role of technicians in this field is to make proposals, final decisions depend on a political assessment that includes other aspects.

Very schematically (the radiation protection principles will provide a more precise framework for these objectives), it is thus a matter of simultaneously:

- ensuring normal facility operating conditions that do not expose workers to excessive radiation nor the release of significant radioactivity by any effluents;
- preventing incidents and accidents;
- limiting the impact on workers, the public and the environment of any incidents and accidents that may occur nonetheless.

This is accomplished by taking appropriate measures in the design, construction, operation and decommissioning of facilities.

For a given type of facility, the process begins by identifying the type of potential risks involved and their magnitude. The means required to ensure safety can only be defined and analysed after this preliminary step has been completed.

France has been involved in building and operating nuclear facilities since the middle of the last century, beginning with small prototype or research reactors as early as the 1950s, followed in the 1960s by power-generating gas-cooled reactors (GCRs), which use natural uranium as fuel and are cooled and neutron-moderated using graphite, and finally, since the 1970s, by 58 pressurized water reactors, first under licence from Westinghouse and later designed by Framatome. The GCRs were all shut down before 2000. Many of the pressurized water reactors in service, however, are now old; the 900 MWe reactors have been in operation for 40 years, the designed lifetime initially planned for certain equipment items.

To gain a clear focus on the purpose of nuclear safety, the biological effects of ionizing radiation and the fundamental principles of the radiological protection system are briefly presented in the first chapter. The reader will then be able to appreciate the magnitude of the consequences of the phenomena under consideration and the serious accidents that occurred at the following nuclear power plants: Three Mile Island in 1979, Chernobyl in 1986 and Fukushima Daiichi in 2011.

Likewise, regulations define how responsibility is shared to ensure safe nuclear practices and to continuously improve nuclear safety. Remaining in a perspective that is more technical than administrative, the second chapter presents the principles of management and relations between the organizations ultimately contributing to safety: facility operators, who are primarily responsible for the safety of their nuclear facilities, safety authorities, technical safety organizations and advisory committees, as well as civil society, whose involvement has increased considerably since the 1970s.

The second part, devoted to taking safety into account in the reactor design phase, first reviews the development of reactors based on the fission of uranium-235 and explains some of the fundamentals of physics applied in pressurized water reactors. This is followed by a description of the general objectives, principles and concepts applicable to PWR design, such as the fundamental safety functions, confinement barriers, the defence-in-depth concept and the deterministic and probabilistic approaches to safety analysis. On all these subjects, more stringent objectives and requirements have been adopted over time as a result of in-depth discussions (sometimes in a European framework) between operators, designers and safety organizations to take into account lessons learned from serious incidents and accidents, especially those at Three Mile Island, Chernobyl and Fukushima Daiichi nuclear power plants, as well as the flooding of the Blayais nuclear power plant in late December 1999. In the 1990s, taking into account the possibility of core-melt situations in the design phase of nuclear power reactors was one of the major issues in the overall improvement of safety in 'next generation' nuclear power reactors such as the European Pressurized water Reactor (EPR). At the same time, the design methods and rules applied to study postulated events using the deterministic approach (loss[2]-of-coolant accidents, reactivity insertion accidents, external hazards, etc.) have been refined, particularly in light of knowledge gained through international research.

The third part deals with some of the most important aspects of 'operational safety' in nuclear power reactors: startup tests carried out before reactors are actually commissioned; feedback from events that occurred during operation, illustrated by a few examples that have provided substantial knowledge; equipment maintenance; and in-service inspections, with some of the most significant anomalies discovered and how they were handled. In this respect, old anomalies or events that affected nuclear power reactors in France during their initial years of operation (and other reactors abroad) have not been omitted due to their educational value, since the recurrence of similar events in one form or another cannot be categorically ruled out. Conversely, recent events or events still under discussion between the operator, the French Nuclear Safety Authority (ASN) and IRSN are deliberately not covered in this book.

With regard to in-service inspections, an entire chapter has been devoted to this topic. The various programmes implemented are the focal point of discussions between Électricité de France (EDF) and safety organizations, as the corporation forecasts extension of the operating lifetime of reactors beyond the 40 years adopted in the design stage. These programmes must provide sufficient assurance that there is adequate management of the ageing[3] of components, particularly those that are difficult or impossible to replace (especially reactor vessels).

The fourth part of the book covers the accidents that occurred at the Three Mile Island, Chernobyl and Fukushima Daiichi nuclear power plants, their consequences (including health issues) and the lessons learned. In brief, these accidents have led to a certain number of concrete measures (involving both equipment systems and organization) aimed at improving the prevention of various situations, including core melt (due, for example, to excessive reactivity insertion, a subject that prompted particularly detailed investigation following the Chernobyl accident), situations involving loss of containment, early or significant release of radioactive substances into the environment, while also taking into account the possibility of external events (earthquake, flooding, etc.) that are more severe than those considered during facility design (or facility safety reassessment). Adopted in France following the Fukushima Daiichi nuclear power plant accident, the concept of a 'hardened safety core' capable of withstanding this type of hazard is explained, with implementation illustrated for reactors in the French nuclear power plant fleet. Measures taken in other countries (Belgium and USA) are also described.

[2] In the field of nuclear safety, the term 'loss' is widely used. It corresponds to a state of unavailability or failure, such as the loss of reactor coolant in the case of a pipe break in the reactor coolant system or the loss of off-site power supplies in the case of failure or unavailability of the power distribution and supply grid of a nuclear power plant, for example.

[3] This term refers to the various processes that alter the state of equipment over time, some of which will be discussed further on, particularly in Chapter 27.

Finally, the measures taken by both public authorities and the operator, EDF, in terms of preparing for and responding to (radiological) emergencies are presented.

The fifth and last part of the book reviews some of the most remarkable contributions of studies and research and development work on reactor safety in French nuclear power plants. The last chapter also presents some of the very many simulation software programs used for safety analyses, preparation of experiments or use of experiment results. Additional information can of course be found in scientific works from Areva NP or Framatome, the French Alternative Energies and Atomic Energy Commission (CEA) and EDF.

Three chapters cover human and organizational factors, a subject that was briefly addressed in various fields in *Elements of Nuclear Safety* (1996). Operating experience feedback, which has led to numerous studies and the development of various approaches in this area, has also earned its place in this book.

Finally, it should be noted that, unless indicated otherwise, the information presented in this book corresponds to the state of knowledge as at late 2019.

Part 1

General Background

Chapter 1

Biological and Health Effects of Ionizing Radiation – The Radiological Protection System

As stated in the introduction, since nuclear facilities, especially reactors, contain significant amounts of radioactive substances, it is appropriate to review certain notions on radioactivity, as well as available knowledge on the biological and health effects of radioactivity. These notions are the basis for achieving an overall assessment of the possible radiological consequences of normal or abnormal situations and for establishing the basic principles of radiation protection.

This chapter, intended as an overview, is based in particular on recommendations from the International Commission on Radiological Protection (ICRP), more specifically ICRP Publication 103, and also presents the radiological effects covered in the book *Radioactive Fallout from the Chernobyl Accident Measured in France*[4].

[4] P. Renaud, D. Champion, J. Brenot, *Les retombées radioactives de l'accident de Tchernobyl sur le territoire français – Conséquences environnementales et exposition des personnes* (Radioactive Fallout from the Chernobyl Accident Measured in France – Consequences on the Environment and Population Exposure), Science and Technology Series, IRSN, *Éditions TEC & DOC*, Lavoisier, 2007.

1.1. Biological and health effects of ionizing radiation

1.1.1. Biological processes

Ionization of an atom, which occurs when a peripheral electron is torn away by a particle or radiation, modifies the atom, at least transiently, and can sometimes damage the cell containing it. If this cellular damage is not properly repaired, it can prevent the cell from surviving or reproducing or, more rarely, result in a viable but altered cell.

A cell with damaged DNA[5] (a gene mutation) that has not been eliminated can, after a fairly long period, lead to cancer. Epidemiological studies show that the probability of cancer occurrence is a function of the dose received. The severity of the cancer, however, is independent of the dose. This is known as a 'stochastic', or random, effect, where the relationship between cause and effect is probabilistic.

If mutations affect germinal cells, there is a risk of hereditary or genetic effects that are also probabilistic. These effects, observed in animals, have never been demonstrated in humans.

If enough cells are destroyed, there will be observable damage appearing as a loss of tissue function. Above a certain level of exposure, called a threshold, the damage will be obvious and its severity will increase as the dose increases. This type of effect is described as deterministic or certain or, more simply, a tissue reaction.

As can be seen, the consequences of radiation exposure are not easy to assess. They can be expressed in terms of the probability of death, which may not occur until decades later, or in terms of certainty of a functional effect or death, if the dose is high enough.

#FOCUS

The different types of ionizing radiation

There are many types of radiation (commonly called 'rays'), that are visible or invisible, but most (radio, mobile phones, microwaves) are not ionizing.

Radiation is an emission of energy or a beam of particles. Certain types of radiation (neutrons, X rays, alpha (α), beta (β) and gamma (γ) rays) are called ionizing radiation because they carry enough energy to transform the atoms they pass through into ions (an atom that has lost or gained one or more electrons). Neutrons can also be absorbed by atomic nuclei. This can make matter unstable.

[5] Deoxyribonucleic acid: biological macromolecule present in all cells as well as in many viruses. DNA contains all the genetic information, known as the genome, necessary for the development, functioning and reproduction of living organisms.

An atom – unstable by nature or after contact with radiation – will try to stabilize itself by emitting different types of radiation:

- by losing protons and neutrons: two protons and two neutrons (helium nucleus) will form α radiation;
- by transforming a neutron into a proton or vice versa: beta minus β^- or beta plus β^+ radiation;
- by emitting photons (particles that make up light): X rays and γ rays;
- by emitting monoenergetic electrons (internal conversion[6]);

or undergo a nuclear fission reaction, leading to the formation of lighter atoms and the emission of neutrons.

Radiation has different effects on the body depending on the type of radiation and the received dose. The energy is not the same for all types of radiation, so the means of protection are different. For example, one sheet of paper is enough to stop alpha radiation, but one metre of concrete or lead is needed to stop gamma radiation (Figure 1.1).

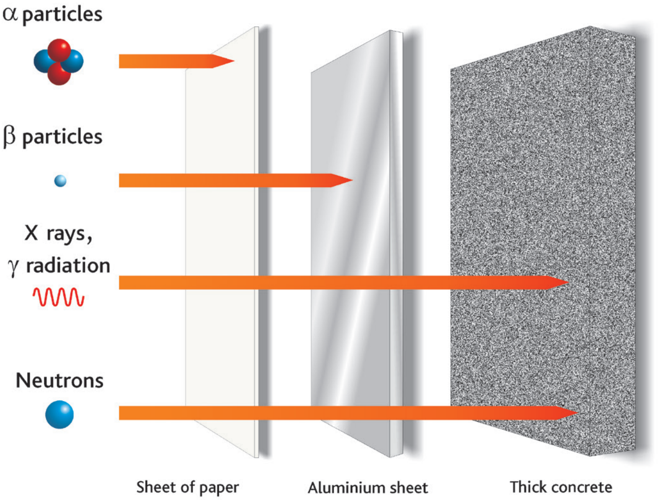


Figure 1.1. Effectiveness of various types of protection against different forms of ionizing radiation. Georges Goué/IRSN.

In nuclear power plants, alpha emitters, which create even greater cellular and molecular damage, pose specific problems in terms of radiation protection for workers (risk of internal contamination) and release to the environment (the concentration of alpha emitters in liquid and gaseous effluents must remain below

[6] See work by Auger, Coster and Kronig.

detection limits, which are set, for each plant, in a decision by ASN, the French Nuclear Safety Authority). If an alpha emitter is found in a contaminated organ or tissue, damage will be significant because the energy deposited locally is very high.

1.1.2. Review of units of measure

The current unit of radioactivity is the becquerel (Bq), equal to 1 decay per second. It is a very small unit and very often prefixes are used to express multiples of magnitude: mega (M) = 10^6, giga (G) = 10^9, tera (T) = 10^{12}, peta (P) = 10^{15} or exa (E) = 10^{18}.

A former unit of measure was the curie (Ci), equal to 37×10^9 decays per second or becquerels. It was historically defined as the activity of one gram of radium-226. As this unit is relatively large, prefixes were used to express reduced magnitude: micro (μ) = 10^{-6}, nano (n) = 10^{-9} and pico (p) = 10^{-12}.

1 Ci = 37×10^9 Bq or 37 GBq; 1 Bq = 27×10^{-12} Ci or 27 pCi.

Two units express the interaction between radiation and the human body.

The gray (Gy) expresses the energy deposited in matter by a particle or by radiation; 1 gray = 1 joule (J)/kilogram (kg) of matter. This is the unit used to measure absorbed dose. The former unit was the rad (1 Gy = 100 rad).

The smaller the distance travelled by the particle when it deposits its energy, the greater will be the potential harmfulness of the absorbed dose. This is known as linear energy transfer (LET) and is expressed in joule/m (or keV/μm). A 'radiation weighting factor' is introduced to determine, for each type of radiation, an 'equivalent dose' to qualify its impact in terms relevant to a reference radiation, X rays or gamma radiation. By convention, the weighting factor is 1 for electrons, X rays and gamma rays. It is 20 for alpha particles and heavy nuclei, and varies from 2.5 to 20 for neutrons, which can reach a maximum energy of the order of one megaelectron volt (MeV).

The sievert (Sv) is the unit of equivalent dose. One sievert is equal to 1 J/kg. The former unit was the rem (1 Sv = 100 rem).

With regard to the different possible effects, each type of tissue and organ has a specific sensitivity to the risk of cancer. For every 100 fatal cancers observed after external whole-body irradiation, there are about 12 lung cancers, four thyroid cancers and one skin cancer, for example, and one does not exclude the other. A 'tissue weighting factor' is thus introduced to convert the equivalent dose to an 'effective dose' (also in Sv) averaged over the whole body. The weighting factor for gonads (ovaries and testes) takes into account the risk of hereditary effects.

In the case of internal contamination, irradiation continues as long as the radionuclide has not been eliminated. It can be eliminated through its own radioactive decay or by excretion. In ten days, half of any tritium ingested is eliminated, whereas it takes about 100 days for caesium. In such a case, the 'committed dose' resulting from contamination is calculated over the next 50 years for workers and up to 70 years for members of the public. By regulation, this dose is 'credited' at the time of contamination.

Both effective and committed doses are expressed in sieverts.

In the remainder of this chapter, the term 'dose' generally refers to the 'effective dose'.

The relationship between one becquerel and the resulting number of grays or sieverts therefore depends on the energy of the particle or radiation and the mode of interaction with the tissues involved and, for internal contamination, the retention time of the radionuclide in the body.

1.1.3. Natural radioactivity

Humanity has always been exposed to a wide spectrum of naturally occurring ionizing radiation. Exposure is due to cosmic radiation, telluric radiation (mainly gamma radiation from potassium-40 and radium-228 and 226), radioactive substances naturally present in the human body from food and water (mainly lead-210, carbon-14 and potassium-40), and inhalation (mainly radon-222).

The annual dose from these natural sources, averaged over the entire population of the world, is between 2 and 3 millisieverts (mSv). Under average exposure conditions, cosmic rays, gamma rays from the ground and ingested substances each contribute approximately 0.3 to 0.4 mSv. The proportion due to radon inhalation is significantly higher, up to 1.3 mSv on average. It varies greatly from place to place and depends, in particular, on soil composition, dwellings and living conditions.

These values cover wide variations and higher local doses can be observed in various locations. Doses from cosmic rays can be up to five times greater in inhabited areas at high altitude. At specific locations, there are annual doses due to terrestrial gamma radiation that can reach up to 100 mSv. The highest annual doses are due to radon, which can approach 1 Sv in extreme cases that have concentrations of several tens of thousands of Bq/m^3.

In France, the average dose received by an individual is within the range of the world average, about 3 mSv/year, due to radon, cosmic and terrestrial radiation and food, but can vary from approximately 1 to 15 mSv/year. Worldwide, the gap may be even greater.

Health risks due to exposure to natural radioactivity have been identified for exposure to radon at concentrations of about 200 Bq/m^3 in dwellings, but this does not mean that there are no risks at lower exposures.

In addition to natural radioactivity, the medical use of radiation for diagnostic purposes in developed countries adds an average individual dose of about 1 mSv per year (3 mSv in the USA and 0.6 mSv for the world average). Voluntary therapeutic exposure, which is generally much higher, is not included in this count.

1.1.4. Health effects

The best sources of information on the effects of ionizing radiation are provided by direct observation of its effect on humans. The Japanese epidemiological Life Span Study (LSS) on the survivors of the Hiroshima and Nagasaki bombings is of particular importance, but it is not the only one. Other epidemiological studies are also used, focused on patients exposed to radiation for medical treatment or diagnosis and on certain groups of workers exposed to radiation due to their occupation or during severe accidents, involving either nuclear facilities or sources for medical or industrial use.

Biological research on micro-organisms, in vitro cultured cells and animals also provides a great deal of additional information on damage mechanisms and dose-effect relationships.

UNSCEAR, the United Nations Scientific Committee on the Effects of Atomic Radiation, keeps a watch on knowledge of the effects of ionizing radiation based on scientifically recognized publications that contribute to understanding the phenomena and help establish a relationship between dose and effect, when possible.

Based on this knowledge, ICRP recommends a general ‘radiological protection system’ and provides detailed updates to the above-mentioned weighting factors required in the system.

ICRP Publication 103 (2007) is the most recent work of a general nature. It proposes a new approach to radiological protection, presented at the end of this chapter, and provides an overview of weighting factors. These factors are reviewed regularly to take into account the evolution of scientific knowledge.

1.1.4.1. Deterministic effects, tissue reactions

Deterministic effects are due to the destruction of a significant proportion of cells in a tissue or organ. For these effects to become observable, the rate of cell destruction must be sufficient to exceed the repair capacity of the tissue or organ. ICRP Publication 118[7] (2012) introduces the expression ‘tissue reaction’ to describe these phenomena.

The extent of these effects increases with the absorbed dose.

For most human organs, the threshold at which significant deterministic effects occur is greater than or equal to 1 Gy, but some effects may occur at 100 mGy. The sensitivity of each individual can also change the threshold level.

Note that at these levels, it is directly the absorbed energy that counts, i.e. just the number of grays, without applying any weighting factors.

Experience provides the following orders of magnitude for whole-body exposure:

[7] ICRP Statement on Tissue Reactions and Early and Late Effects of Radiation in Normal Tissues and Organs – Threshold Doses for Tissue Reactions in a Radiation Protection Context, ICRP Publication 118, Ann. ICRP 41(1/2), 2012.

- above 0.1 Gy, temporary male sterility, temporary degradation of the blood count;
- above 1 Gy, faintness, nausea, great fatigue, immunosuppressive effect with risk of infection;
- above 2 Gy, skin erythema, loss of hair and body hair, significant degradation of the blood count, death in about 5% of the people concerned within a few months;
- from 3.3 to 4.5 Gy, the mortality rate is 50%;
- above 5 Gy, radiological burns of increasing severity;
- about 6 Gy, gastrointestinal damage with risk of internal bleeding;
- for 8 Gy, lung damage with a mortality rate of around 95% in a few weeks;
- from 15 to 20 Gy, coma, brain death, rapid death.

Erythema and skin burns can occur even with local exposure, as observed on early radiologists.

The threshold of occurrence for cataracts has recently been reassessed. ICRP Publication 118 (2012) now retains the value of 0.5 Gy, which is ten times less than the value previously retained for either single or fractionated exposure.

1.1.4.2. Stochastic or random effects

Stochastic (probabilistic or random) effects occur in cells where the DNA has been damaged due to interaction with ionizing radiation and has not recovered well, resulting in gene mutation.

These situations most often lead to cancers where the severity is unrelated to the level of exposure.

These cancers occur more frequently in a group that has been exposed than in a group that has not. Within the group of people exposed, the difference in the occurrence of cancer increases as the difference between doses rises. Nevertheless, it is currently impossible to distinguish a radiation-induced cancer from a cancer related to another risk factor or to predict who in the exposed group will develop the disease.

Epidemiological and experimental studies prove that the risk of developing a cancer exists for doses of 100 mSv and even lower. As will be seen in Section 1.1.5, the number of deaths from spontaneous cancers and the relative variability of this number from one year to the next imply that epidemiology cannot be used to determine whether or not this risk exists for significantly lower doses.

Knowledge of basic cellular processes, coupled with data on dose-effect relationships, supports the view that in the low dose range, below approximately 100 mSv, it is scientifically plausible that the incidence of carcinogenic effects may increase linearly with the dose received.

ICRP retains that, **given current knowledge, with a view to protection and regulation, therefore in a prudent approach, it is advisable to retain a linear relationship without a threshold between dose and stochastic effects**. The dose-effect model adopted is known as the Linear No-Threshold (LNT) model and applies to cancers and hereditary diseases.

'Nominal risk coefficients' express the lifetime excess absolute risk[8] for a group of 100 people receiving a dose of 1 Sv. They have been reassessed since the previous ICRP publication in 1990 (ICRP Publication 60); the decrease is slight for cancers and significant for hereditary effects (Table 1.1). As there are no clearly demonstrated hereditary effects on humans, estimates are based on animal experimentation. The very broad spectrum of severity of genetic disorders makes it difficult to define a coefficient of proportionality; for impairments considered as 'severe', ICRP Publication 103 applies a coefficient of 0.2% per sievert for the entire population.

Table 1.1. Nominal risk coefficients in 10^{-2}/Sv at low dose rates.

Exposed population	Cancer		Hereditary effects		Total	
	ICRP 60 (1990)	ICRP 103 (2007)	ICRP 60 (1990)	ICRP 103 (2007)	ICRP 60 (1990)	ICRP 103 (2007)
Whole group	6.0	5.5	1.3	0.2	7.3	5.7
Adults	4.8	4.1	0.8	0.1	5.6	4.2

This model provides a prudent basis for the practical needs of preventive radiation protection. The presence of decimals is not important and ICRP suggests using an overall factor of 5%/Sv. Nonetheless, ICRP considers that it would be inappropriate to use this factor to calculate a hypothetical number of cancer cases or hereditary diseases that could be associated with very low doses received by a large number of people over very long time periods, for example as the result of an accident.

Radiation-induced cancers occur after a fairly long latency period and deaths occur beginning about five years after exposure and then continue over several decades, particularly for 'solid' cancers. Studies conducted on Japanese survivors of the atomic bombings at Hiroshima and Nagasaki showed that, at the beginning of systematic studies, five years after the explosions, the peak of mortality from leukaemia ('liquid' cancer) had already been passed.

The 'epidemic' of thyroid cancers in children living in the areas near Chernobyl most affected by plumes and deposits resulting from the accident showed that similar time periods also apply to the occurrence of this type of cancer. It will be seen in Chapter 34 on the Chernobyl accident that, although these cancers are numerous, the number of deaths caused by them can nonetheless be considered low.

[8] In epidemiology, absolute risk is an indicator of the frequency of a pathology or health event in a given population. An absolute risk is often expressed as the number of cases per 10,000 people. This is usually referred to as prevalence (total number of cases) or incidence rate (number of new cases).

1.1.4.3. Induction of diseases other than cancer

In-utero exposure can affect the fetus. After the first weeks of pregnancy and particularly during the last trimester, a dose of more than 0.1 Gy received by the fetus can hinder its development and can affect the child's IQ.

ICRP Publication 118 reviews the effects of radiation on various tissues and organs of the human body in the short, medium and long term. It covers the immune, haematopoietic (blood cell production system), digestive, reproductive, respiratory, urinary, muscular, skeletal, nervous and cardiovascular systems, as well as the skin and eyes.

Adding the cardiovascular system to this list is a significant new development, and recognizes that serious disorders of this system can occur in the medium to long term following radiation exposure. It involves a tissue reaction and the adopted threshold is 0.5 Gy, for either single or fractionated exposure. The question has been asked since the 1990s, but recent review studies (including those by Mark P. Little et al. 2008, 2010 and Ozasa et al.[9], 2012) have contributed to this conclusion, which is well documented in the scientific literature.

Another significant development involves the threshold of eye exposure that could cause cataracts, which has been reduced by a factor of 10. The reference value is now 0.5 Gy.

After a systematic review and meta-analysis of the available data, Mark P. Little and 37 other specialists[10] suggest that non-cancerous pathologies caused by exposure to ionizing radiation could result in as many premature deaths as cancers.

The latter estimates are not included in ICRP Publication 118.

1.1.5. Example of the limitations of epidemiology

It is possible to illustrate the limits of epidemiology using French data on populations and their mortality, particularly death from cancer.

From 1979 to 2010, France's population rose fairly steadily from 53,482,000 to 62,765,000[11] (see Figure 1.2). At the same time, the number of deaths per year decreased from 540,000 to 530,000[12], but with large annual variations, marking the increase in life expectancy.

[9] Ozasa et al., Studies of the Mortality of Atomic Bomb Survivors, Report 14, 1950-2003: An Overview of Cancer and Noncancer Diseases, Radiation Research, 177(3):229-243, 2012.

[10] M. P. Little et al., Systematic Review and Meta-analysis of Circulatory Disease from Exposure to Low-Level Ionizing Radiation and Estimates of Potential Population Mortality Risks, Environmental Health Perspectives, 120:11, November 2012.

[11] INSEE data rounded to the nearest thousand.

[12] INSERM, *Causes médicales des décès* (Medical Causes of Death), https://www.cepidc.inserm.fr/.

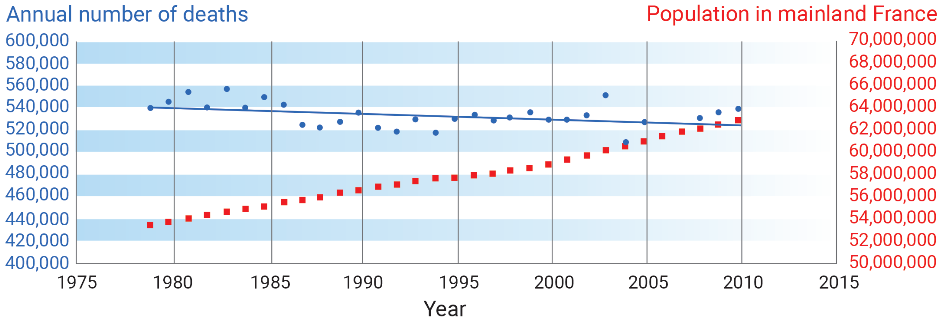


Figure 1.2. Population of mainland France and annual mortality. IRSN.

The website of the French National Institute of Health and Medical Research (INSERM) indicates the number of deaths by cause, age and gender, making it possible to track the number and rate of deaths due to cancer (International Classification of Diseases, ICD 10, codes C00 to C97).

Cancer is the cause of one-third of deaths, more for men than women, with the number of deaths for men relatively stable since 1995 (see Figure 1.3). Despite these high figures, annual fluctuations exceed ±1%.

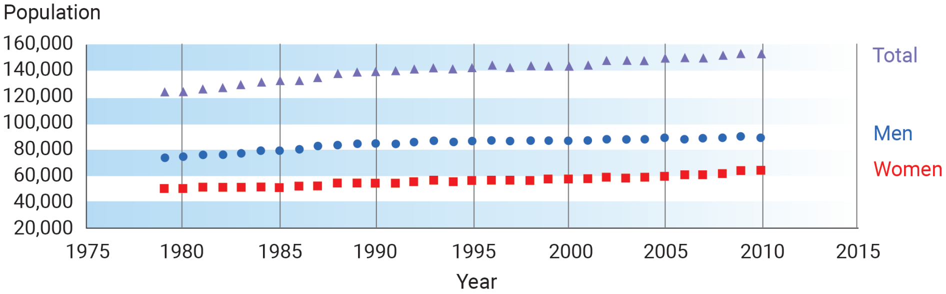


Figure 1.3. Annual number of cancer deaths in mainland France. IRSN.

Exposure of 600,000 people, i.e. 1% of the population, to a dose of 10 mSv could cause up to 300 additional deaths by cancer, some of which would take place after a few years, with most others occurring 20 to 50 years later, while 'spontaneous' cancers would result in about 16,000 deaths. It would not be possible to distinguish the additional rise in cancer caused by exposure.

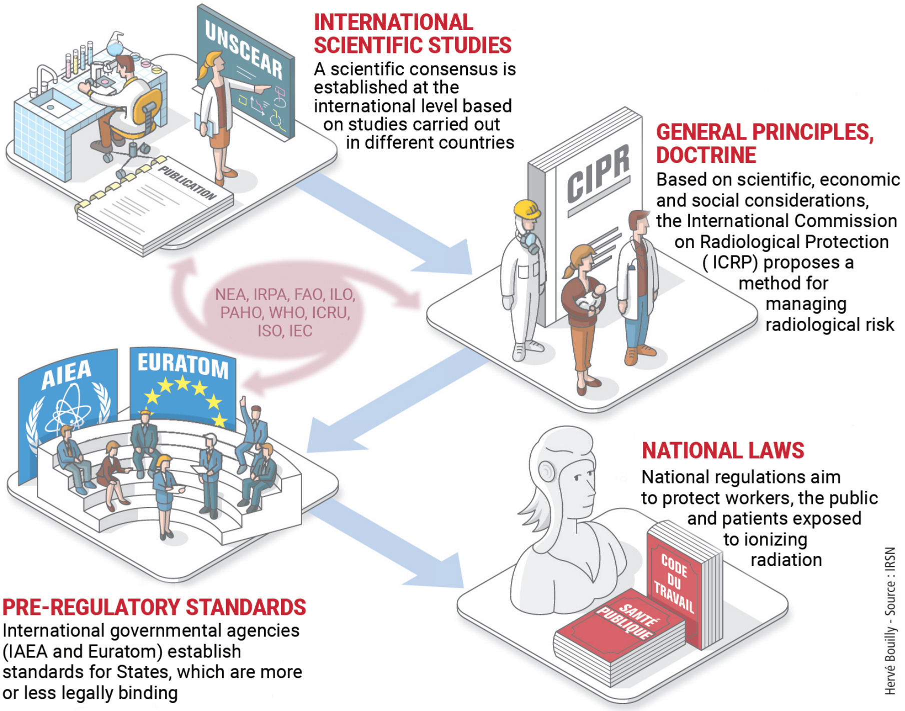
For rare spontaneous cancers such as thyroid cancer in children, the detection threshold may be lower, but it would not be possible to distinguish radiation-induced cancers from others.

1.2. Radiological protection system

The numerous cases of leukaemia observed among radiologists starting in the late 1920s – which lasted until the 1950s – gave rise to a collective awareness of the effects of ionizing radiation. At the Second International Congress of Radiology in Stockholm held in 1928, it was decided to create the International X-ray and Radium Protection Committee, which in 1950 became the International Commission on Radiological Protection (ICRP).

The ICRP created the 'radiological protection system' (see Figure 1.4). The main purpose of this system is to contribute to an appropriate level of protection for people and the environment against the harmful effects of exposure to ionizing radiation, without unduly limiting useful human activities that could lead to such exposure. With regard to human health, the aim is to control exposure to ionizing radiation in order to prevent deterministic effects and reduce stochastic effects, keeping them within reasonable limits.

To achieve this, ICRP Publication 103 (2007) recommends a workable and structured approach with three types of exposure situations, three exposure categories and appropriate application of three radiation protection principles.



INTERNATIONAL SCIENTIFIC STUDIES
A scientific consensus is established at the international level based on studies carried out in different countries

GENERAL PRINCIPLES, DOCTRINE
Based on scientific, economic and social considerations, the International Commission on Radiological Protection (ICRP) proposes a method for managing radiological risk

PRE-REGULATORY STANDARDS
International governmental agencies (IAEA and Euratom) establish standards for States, which are more or less legally binding

NATIONAL LAWS
National regulations aim to protect workers, the public and patients exposed to ionizing radiation

Hervé Bouilly - Source : IRSN

Figure 1.4. How radiation protection rules are defined.

1.2.1. Types of exposure situations

Exposure situations are very diverse. In each situation, the starting point is a source of radiation that exposes individuals to radiation via different exposure pathways. The system of radiological protection applies to controllable sources of radiation, whether naturally occurring or man-made. The type of source is important in choosing the protection system, as it results in three distinct types of exposure situations.

Existing exposure situations: the source is present prior to the decision to place it under control. This is the case for most natural sources of radiation: radon, cosmic radiation, radiation from the ground. This is also the case for legacy radiation from industry (contaminated sites), or the consequences of a radiological emergency, i.e. an accident situation resulting in the release of radioactive substances.

Existing exposure situations are chronic exposure situations managed by controlling exposure pathways rather than the source itself, which is not always easy.

Another type of situation corresponds to **planned exposure situations**: the deliberate introduction and use of a radiation source, for example to generate electricity, treat patients or inspect a weld. The source is generally man-made, but can also be natural. In planned exposure situations, the source is introduced deliberately. It is therefore assumed to be controlled from the source design phase to its disposal. This case corresponds to the various aspects of normally operating facilities using duly authorized radioactive sources of any kind.

The last type of situation pertains to **emergency exposure situations**, which may occur when there is loss of control of a radiation source used in a planned exposure situation, or as the result of a malicious act or any other unexpected situation. It requires urgent action in order to avoid or at least reduce undesirable consequences.

1.2.2. Exposure categories

The ICRP makes a distinction between three categories of exposure.

Medical exposure: the exposure of patients for diagnosis, surgery or therapy. Exposure is intentional and directly benefits the patient. The characteristics of medical radiological practices, especially the physician-patient relationship, require a different approach than those applied to other planned exposure situations.

Occupational exposure: this refers to exposure to any type of radiation received by workers in the course of their professional activity. However, because of the ubiquity of radiation, and to avoid having to subject all workers to a radiological protection regime, the definition of 'occupational exposure' is limited to radiation exposure incurred at work that can reasonably be considered as being the responsibility of the operating management.

Public exposure: this refers to all exposures that are neither medical nor professional.

The types of exposure situations and exposure categories can be presented in the form of a matrix that determines the structure of the radiological protection system. Although the system is applied uniformly, it is implemented in a way that can adapt to each case. Therefore, a given individual exposed to radiation as a member of the public, as a patient or as a worker is managed in a different way, according to the type of exposure situation.

Exposure management is based on the application of three principles: justification, optimization and limitation.

1.2.3. Justification principle

Any decision that changes a radiation exposure situation must do more good than harm. The justification principle, related to the ethical value of beneficence/non-maleficence[13], is not specific to facilities or activities that create or use ionizing radiation. The risk of exposure to ionizing radiation may be combined with other risks. Any activity involving potential harm to humans, especially the workers involved, and their environment must be subject to an assessment of its advantages and disadvantages.

The justification principle for radiation protection applies in all three types of exposure situations.

A list of activities using radiation sources considered as justified is established and updated at the national level[14]. Persons who are responsible for an activity that is not on the list must demonstrate that their activity complies with the justification principle. The relevant information is gathered within the framework of the authorization procedure carried out by the public authority on the basis of the file submitted by the applicant and consultation, if necessary, with the public.

Once the project has been justified and authorized, the facility operator is responsible for complying with the commitments made in its application and for meeting any imposed requirements.

The medical exposure of patients is defined in a specific three-step approach. In the first step, the medical use of radiation is generally considered to be justified, given the current state of available care techniques. The second step involves justifying a specific medical radiological practice; this is all the more important as techniques and equipment evolve very quickly. This aspect of the justification of medical exposure is handled in consultation with the relevant professional organizations. Finally, justifying the implementation of a medical radiological procedure on a particular patient is essentially the responsibility of the patient's physician.

In the case of an emergency or existing exposure situation, it is the implementation of a protection strategy that must be justified.

[13] See the recent ICRP Publication 138, Ethical Foundations of the System of Radiological Protection, 2018.

[14] In compliance with Article L.1333-9 of the French Public Health Code.

Some exposures are considered as unjustified. This includes deliberately adding radioactive substances to consumer products such as food, beverages, cosmetics, toys, jewellery or personal ornaments. Any unjustified exposure is prohibited.

1.2.4. Optimization (ALARA) principle

The optimization principle in radiation protection is at the heart of the radiological protection system. It aims to achieve the best possible level of protection given the circumstances. It applies to all exposure situations – existing exposure situations, planned exposure situations and emergency exposure situations – where the justification principle has been applied. It is based on the assumption that a linear dose-effect relationship with no threshold applies at low doses and thus reflects the desire to remain prudent in the absence of scientific proof (the ethical value of prudence).

The optimization of protection is defined as the source-related process that ensures that individual doses, the number of people exposed and the likelihood of unplanned exposure remain **as low as reasonably achievable**[15], given economic and social factors. Any operation leading to exposure must be prepared in advance (insofar as possible in emergency situations), by incorporating foreseeable potential hazards. Optimization continues during and after the operation in question (based on operating experience feedback).

The main stages consist of the following:

- assessing the exposure situation, including potential exposure - these are the ones that could occur if the operation does not take place as planned;
- selecting an appropriate upper limit to restrict doses;
- identifying possible protection options;
- selecting the best option given the circumstances;
- implementing the chosen option;
- assessing the results;
- using lessons learned for future operations of the same type.

The optimization process is applied in a systematic, structured, continuous and iterative manner that aims to cover all relevant aspects. It is based on methods that combine quantitative and qualitative aspects and requires judgements.

Optimization is a state of mind that leads to systematically asking whether everything that is reasonably possible has been done to reduce doses. In a professional context, it requires a commitment from everyone involved, and at all levels. For cases of exposure of members of the public, it requires the involvement of all stakeholders. Optimizing protection also requires adequate procedures and resources.

[15] The 'ALARA' principle, taken from the science of risk management, was formulated for the first time in 1977 by the ICRP in its Publication 26.

The best option is always specific to an exposure situation. Therefore, it is not relevant to set a dose level below which the optimization process should stop.

Optimizing radiological protection does not mean minimizing doses. Optimized protection is the result of an assessment and dialogue, in which the risks of anticipated exposure are compared with the resources available for personal protection. The best option is not necessarily the one with the lowest doses.

Moreover, radiation protection is not only about individual exposure levels; the number of people exposed must also be taken into account. The collective effective dose is a key parameter in optimizing worker protection. During the optimization process, when comparing protection options, careful consideration should be given to the characteristics of the distribution of individual exposure levels within the exposed population.

To ensure that exposed persons are all treated fairly, the radiological protection system provides for restricting individual doses by setting an upper boundary in the optimization process, which is determined on a case-by-case basis. A similar approach can also be applied to collective doses.

In the optimization process, the upper boundary for an individual dose relative to a given source is called the **dose constraint** in planned exposure situations and the **reference level** in other exposure situations (existing or emergency exposure situations).

▶ Dose constraint

A dose constraint is specific to a source. It is used when the source is under control from the outset, the exposure routes are under control and exposure levels are largely predictable. This is the case in planned exposure situations.

It is assumed that the dose constraint must not be exceeded. A dose constraint is not intended, however, to become a regulatory threshold; exceeding it should raise questions, at least within the organization responsible for the source.

The concept of dose constraint was introduced in ICRP Publication 60 in order to avoid disparities in the distribution of individual doses.

▶ Reference levels

Reference levels pertain to emergency and existing exposure situations.

In these situations, it is more difficult to control exposure and the state of the source is imposed on those responsible for radiation protection at the beginning of the optimization process. A reference level is used as a basis for response management, but it is primarily an indicator. Under these conditions, and given the prevailing circumstances of exposure (unexpected situations), not all doses will necessarily be lower than the previously set reference level, even at the end of the optimization process, depending on the success of the strategy.

In planning, the dose constraint and the reference level are used in the same way. They represent the individual dose level, **induced by a source,** which must not be reached or exceeded. This is therefore a dose level above which protection is unlikely to be optimized. The value chosen depends on the circumstances of the exposure situation under consideration. In practice, protection options that do not bring doses below this value are, in theory, considered insufficient.

A difference in use appears retrospectively, i.e. once the optimization process has been implemented. In the case of a planned exposure situation, the source and exposure pathways are controlled and exposures are largely predictable, so that the predefined dose constraint should not be exceeded, even if it does not constitute a limit; exceeding it should logically call for investigating the causes and reporting the lessons learned.

In emergency or existing exposure situations, however, it is more difficult to control the situation. As mentioned above, the state of the source is imposed on those responsible for radiation protection from the beginning of the optimization process. Under these conditions and given the prevailing circumstances, even at the end of the optimization process, not all doses will necessarily be lower than the predefined reference level. The tail of the distribution curve of individual doses may even show high doses, depending on the circumstances and the behaviour of individuals. The reference level will therefore serve as a benchmark for assessing performance retrospectively and the optimization process will be pursued as long as possible to reduce the number of individuals whose doses remain above the reference level.

Neither dose constraints nor reference levels represent a demarcation between ‘safe’ and ‘dangerous’. It is important to note that optimizing protection aims to reduce exposure to a level as low as reasonably achievable regardless of the initial level of exposure. Thus, the optimization process must be pursued even if doses are below the dose constraint or reference level, as long as its implementation appears reasonable.

Dose constraints and reference levels are therefore primarily optimization tools. For medical imaging procedures, the relevant tool is the ‘diagnostic reference level’, which indicates whether, under routine conditions, the levels of patient dose are above or below the median level for the procedure in question.

▶ Choosing dose constraints and reference levels

The ICRP provides guidance for choosing the value of a dose constraint or reference level depending on the characteristics of the situation and protective actions required (see Table 1.2).

First of all, it considers that a dose higher than a value of about 100 mSv incurred either acutely or over a year almost always justifies the implementation of protective actions. Consequently, it is not appropriate to choose a dose constraint or reference level that would be higher than this value in any situation.

Table 1.2. Table from ICRP Publication 103.

Bands of constraints and reference levels[a] (mSv)	Characteristics of the exposure situation	Radiological protection requirements	Examples
Greater than 20 to 100[b, c]	Individuals exposed by sources that are not controllable, or where actions to reduce doses would be disproportionately disruptive. Exposures are usually controlled by action on the exposure pathways.	Consideration should be given to reducing doses. Increasing efforts should be made to reduce doses as they approach 100 mSv. Individuals should receive information on radiation risk and on the actions to reduce doses. Assessment of individual doses should be undertaken.	Reference level set for the highest planned residual dose from a radiological emergency.
Greater than 1 to 20	Individuals will usually receive benefit from the exposure situation but not necessarily from the exposure itself. Exposures may be controlled at source or, alternatively, by action in the exposure pathways.	Where possible, general information should be made available to enable individuals to reduce their doses. For planned situations, individual assessment of exposure and training should take place.	Constraints set for occupational exposure in planned situations. Constraints set for comforters and carers of patients treated with radiopharmaceuticals. Reference level for the highest planned residual dose from radon in dwellings.
1 or less	Individuals are exposed to a source that gives them little or no individual benefit but benefits to society in general. Exposures are usually controlled by action taken directly on the source for which radiological protection requirements can be planned in advance.	General information on the level of exposure should be made available. Periodic checks should be made on the exposure pathways as to the level of exposure.	Constraints set for public exposure in planned situations.

a : acute or annual dose.

b : in exceptional situations, informed volunteer workers may receive doses above this band to save lives, prevent severe radiation-induced health effects, or prevent the development of catastrophic conditions.

c : situations in which the dose threshold for deterministic effects in relevant organs or tissues could be exceeded should always require action.

Table 5. Framework for source-related dose constraints and reference levels with examples of constraints for workers and the public from single dominant sources for all exposure situations that can be controlled.

This dose of 100 mSv corresponds to a nominal increase in the probability of cancer of 5 per 1000, based on the linear no-threshold relationship between exposure and stochastic effects. It corresponds to the threshold at which initial tissue reactions appear in the most sensitive individuals, reactions which are all transitory at this level. It is therefore not a level marking the boundary between a safe situation and a dangerous one.

Below 100 mSv, ICRP makes a distinction between three bands corresponding to exposure situations having the same characteristics: less than 1 mSv, 1 to 20 mSv and 20 to 100 mSv. The time period taken into account depends on the situation. It is usually a year. For workers, the dose constraint can be defined according to the time required to perform a specific action. The main characteristics that determine how an exposure situation is positioned on the defined dose bands are the degree of difficulty in controlling the source, the protective actions that the situation requires for exposed persons (training, protective equipment, dose monitoring, etc.) and the benefit derived from the exposure situation, whether individual or societal.

The notion of benefit gained from an exposure situation is assessed for each situation. The only case where the exposed person clearly benefits from the exposure itself is the patient treated through radiation therapy. In all other cases, benefit is derived from the exposure situation either by the exposed person or by society as a whole. The benefit derived from the situation is personal in the case of a patient who receives a diagnostic X ray or in the case of an occupationally exposed worker, for example. It is societal in the case of industrial or medical facilities that discharge effluents, leading to controlled exposure of part of the population. When exposed to naturally occurring radioactivity, the benefit for exposed individuals is generally related to their lifestyle (taking a plane, even if it exposes people to cosmic radiation; attachment to one's region or home, even in the presence of radon; a taste for shellfish, even if they have a higher concentration of radioactivity than other foods). In the case of radioactive contamination, no one benefits from the situation, which is why compensatory measures are taken for exposed persons, in terms of prevention (various restrictions), protection (exclusion zone, protective actions, remediation, technical or psychological support, etc.) and even compensation (indemnification).

For personnel operating and maintaining radioactive sources under normal conditions, a dose constraint in the range of 1 to 20 mSv must be chosen for each operation. However, the regulatory dose limits (see Section 1.2.5 below) must be observed for each individual and for all the individual's activities. These persons benefit from appropriate protection and training as well as individual dose and health monitoring.

In radiological emergencies, i.e. in more or less severe accident situations, the source is no longer under control and it is no longer possible to seek the same level of protection. It is only possible to act on exposure pathways and exposure time. The reference levels that correspond to this situation may be in the highest band (20 to 100 mSv).

However, in order to remain within exposure values close to 20 mSv for members of the public, the latter may be evacuated or subject to dietary restrictions (including leafy vegetables, milk and its derivatives, mushrooms, game, local fish) or restricted activity.

For personnel intervening in the damaged facility, it is the equipment and intervention time that will make it possible to limit exposure.

Given that urgent decisions must be made in these situations, equipment and measuring instruments operating within the appropriate ranges must be immediately available. This means that discussions must take place before the event to consider the possibility of highly degraded situations and procure the necessary equipment for each facility.

It is not the people working inside or outside the facility who will benefit from the action, but society in general, if the action reduces release to the environment. Response teams must therefore be fully informed of the risks involved, and freely and explicitly express their willingness to participate. This involves professionals from outside the facility, such as firefighters, who would be called in to take action.

1.2.5. Principle of application of dose limits

The application of dose limits also aims to ensure a degree of fairness between exposed persons in a context where sources are controlled and exposures can be anticipated. However, while the dose constraint is specific to a given source, **the dose limit applies to an individual** who may be exposed to several sources. Compliance with dose limits ensures that no tissue effects occur and avoids taking an unacceptable risk of stochastic effects for an individual. Other than medical exposure as a patient, the total dose to any individual from all sources authorized through a regulatory process relevant to situations of planned exposure (foreseen during the authorization processes as part of normal operating conditions) must not exceed the appropriate limits. **In practice, the limitation applies only to doses received with certainty in the context of planned exposure situations.**

Since these situations must be fully controlled, dose limits are intended to be included in national regulations as levels which, if exceeded, are in violation of regulations. Values have remained unchanged since the issue of ICRP Publication 60 in 1991, except for the equivalent dose limit for the lens of the eye; the new value recommended by ICRP in 2011 for workers (20 mSv/year instead of 150 mSv/year) was introduced in the new EURATOM Directive on Basic Safety Standards in Radiation Protection (2013/59/EURATOM) (Table 1.3).

Table 1.3. Dose limits recommended by ICRP for planned exposure situations.

Type of limit	Worker	Public
Effective dose	20 mSv per year, averaged over 5 years	1 mSv/year
Equivalent dose for: **– lens of the eye** **– skin** **– hands and feet**	 20 mSv/year 500 mSv/year 500 mSv/year	 15 mSv/year 50 mSv/year –

The above recommended values were introduced in French regulations in 2018 (in the French Public Health Code, Labour Code and Environmental Code), with less flexibility for the occupational dose limit, which is 20 mSv over 12 consecutive months.

Experience shows that dose limits are rarely exceeded in planned exposure situations (i.e. things are as they should be), and that, on average, actual exposures are about an order of magnitude lower than the relevant dose limit. In practice, then, radiation protection essentially consists of implementing the principle of optimization, whatever the exposure situation.

Videos available for viewing

L'échelle des doses de rayonnement (Radiation Dose Bands) (in French)

The Effects of Radiation on our Health

The First Steps Towards Radiation Protection

The Alchemists' Crucible

Chapter 2
Organization of Nuclear Safety Control and Regulation for Nuclear Facilities and Activities in France

2.1. From the founding of CEA to the TSN Act

In France, the organization of nuclear safety control for nuclear facilities and activities, exercised by the State as part of its mission to protect individuals and property, has evolved over time[16]. In the 1950s, it relied on the French Atomic Energy

[16] For further information on the topics covered in this chapter, the reader may refer to works by: P. Saint Raymond, *Une longue marche vers l'indépendance et la transparence. L'histoire de l'Autorité de sûreté nucléaire française* (A Long March to Independence and Transparency. History of the French Nuclear Safety Authority), *La Documentation française*, 2012; C. Foasso, P.I.E. Peter Lang, *Atomes sous surveillance* (Atoms Under Surveillance), 2012; A.-C. Lacoste, *Comment contrôler la sûreté nucléaire en l'absence de règlementation?* (How Can Nuclear Safety Be Controlled Without Regulations?), *Contrôle Review* No. 197, 2014; and P. Saint Raymond, *La règlementation des INB, une longue marche* (Regulating Basic Nuclear Installations: a Long March), *Contrôle Review* No. 197, 2014. Certain information in this chapter is taken directly from these sources. Other noteworthy sources: C. Foasso, *Histoire de la sûreté de l'énergie nucléaire civile en France (1945-2000)* [History of Civil Nuclear Power Safety in France (1945-2000)], doctoral thesis, 28 October 2003, and S. Topçu, *Les physiciens dans le mouvement antinucléaire: entre science, expertise et politique* (Physicists in the Anti-nuclear Movement: Between Science, Expertise and Politics), in *Cahiers d'histoire. Revue d'histoire critique*, 102|2007.

Commission (*Commissariat à l'énergie atomique*, CEA), created in 1945 to take charge of developing all the areas that needed to be covered in order to use nuclear energy.

The initial focus of attention was radiation protection. For this purpose, in 1951, CEA's Radiation Protection Department (*Service de protection contre les radiations*, SPR) was created. The first person to head this department was Dr Henri Jammet, who was responsible for establishing radiation protection measures. Then, faced with the growing use of radioactive sources outside CEA, particularly in the medical field, the Interministerial Commission for Artificial Radioelements (*Commission interministérielle des* radioéléments *artificiels*, CIREA) was created in May 1954. Subsequently, the Central Service for Protection against Ionizing Radiation (*Service central de protection contre les rayonnements ionisants*, SCPRI), administered by the Ministry of Health, was created by the Order of 13 November 1956, with Professor Pierre Pellerin as its director.

In 1958, the Chairperson of CEA founded the Atomic Pile Safety Group, headed by Jean Bourgeois who proposed the creation of a Committee on the Safety of Atomic Installations (*Comité de la sécurité des installations atomiques*, CSIA), which became the Commission on the Safety of Atomic Installations (*Commission de la sécurité des installations atomiques,* CSIA) created on 1 January 1960 and chaired by the High Commissioner for Atomic Energy, Francis Perrin[17]. Two subcommittees were subsequently created, one for atomic piles (*Sous-commission de sûreté des piles*, SCSP), the other for 'critical mass'.

Two weeks after the creation of the subcommittee on atomic piles, the Office of the High Commissioner for Atomic Energy released a list of the atomic pile safety documents that operators were required to prepare for review by an SCSP working group, the Technical Group on Atomic Pile Safety. The safety review thus became a prerequisite for building and commissioning all nuclear reactors. A 'Preliminary Safety Analysis Report'[18] was to be prepared in order to issue a 'safety certificate', required to build any new atomic pile. Once construction was completed, when it was time for plant acceptance tests with the supplier, the person in charge of a pile then had to prepare a report on the pile safety and a draft version of operating instructions, both documents required to issue an 'operating licence'. As part of compliance, managers of atomic piles already in operation had to provide the two documents mentioned above, along with a copy of reports on any major incidents that had occurred since the piles had been set into operation. The expected content of the safety analysis reports was already largely defined, in particular the concept of multiple 'barriers' used between radioactive substances and the environment and the notion of 'maximum possible accident' derived from American practices. The CSIA and SCSP examined the safety analysis reports of the various CEA piles. They were also called upon later for projects

[17] He succeeded Frédéric Joliot-Curie.

[18] These three terms or expressions are those used by C. Foasso in his book, *Atomes sous surveillance*, mentioned in footnote 16.

involving the first nuclear power gas-cooled reactors (natural uranium reactors cooled with carbon dioxide gas, using graphite as the moderator), as well as France's first pressurized water reactor, Chooz A, in the Ardennes area in north-eastern France.

However, it was not until August 1961 that a law on 'the fight against air pollution and odours' (amending the law of 15 December 1917 on hazardous, insanitary or troublesome facilities) introduced the concept of 'nuclear facility'. When the Euratom Treaty of 1957 followed by the Paris Convention[19] in 1960 were signed, it became necessary to at least keep an inventory of this type of facility.

Decree 63-1228 of 11 December 1963, adopted in application of this law, laid the foundation for regulating 'basic nuclear installations' by defining these facilities and requiring that an authorization be granted by decree (thus a government act)[20] before this type of facility could be built ; the corresponding procedure provided for consultation of a new national commission, the Interministerial Commission for Basic Nuclear Installations (*Commission interministérielle des installations nucléaires de base*, CIINB), as well as approval from the Minister of Health. Inspectors were made responsible for inspecting 'hazardous, insanitary and troublesome facilities' to ensure compliance with regulations. To remedy the situation, existing facilities submitted a simple declaration to the Minister in charge of Atomic Energy.

The above decree was amended on several occasions until it was repealed by Decree 2007-1557 of 2 November 2007.

Decree 73-278 of 13 March 1973 created a government agency specifically responsible for nuclear safety. This was the Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN), then part of the Ministry of Industry. The creation of this entity reinforced the State's role as inspector in the development of the French nuclear power programme. Besides, around the same time, the USA created the Nuclear Regulatory Commission (NRC) so that the function of developing nuclear energy facilities was clearly separated from the function of inspecting them. In 1991, the SCSIN became a ministerial directorate (reporting to two ministers), the Directorate for the Safety of Nuclear Installations (*Direction de la sûreté des installations nucléaires*, DSIN), with the same remit. Then, in 2002, by Decree 2002-255 of 22 February 2002, the Directorate General for Nuclear Safety and Radiation Protection (*Direction générale de la sûreté nucléaire et de la radioprotection*, DGSNR) was created, reporting to three ministers, whose remit covered not only the safety of nuclear facilities, but also the regulatory activities of the Directorate General for Health (*Direction générale de la santé*) and the Office for Protection against Ionizing Radiation (*Office de protection contre les rayonnements ionisants*, OPRI) – created in 1994 from SCPRI – and the Interministerial Commission for Artificial Radioelements

[19] Convention on Third-Party Liability in the Field of Nuclear Energy (Paris Convention) of 29 July 1960, amended on 28 January 1964 and 16 November 1982.

[20] It should be noted that industrial facilities classified for environmental protection reasons required simply making a declaration to the Prefect or obtaining an authorization from this authority.

(*Commission Interministérielle des radioéléments artificiels*, CIREA), created – as mentioned above – in 1954 to comply with the Act of 19 July 1952 of the French Pharmacy Code regulating the production, import and use of man-made radionuclides). The DGSNR's missions, specified in the decree referred to above, include:

– "preparing and implementing all measures relating to the safety of basic nuclear installations, in particular by defining the relevant technical regulations and ensuring they are enforced;

– preparing and implementing, in cooperation with other competent administrations, all measures intended to prevent or mitigate the health risks associated with exposure to ionizing radiation, in particular by formulating technical regulations on radiation protection (except for regulations on protecting workers from ionizing radiation) and ensuring they are enforced;

– organizing inspections relating to safety and radiation protection" (for basic nuclear installations as well as industrial and medical facilities);

– "organizing continuous oversight of radiation protection, particularly radiological monitoring of the environment throughout the entire country;

– monitoring discharges of gaseous effluent, liquid effluent and waste from basic nuclear installations;

– participating, in cooperation with other competent administrations, especially civil protection agencies, in the definition and implementation of a technical emergency response in the event of an accident at a nuclear facility [...], or more generally any accident likely to affect human health due to exposure to ionizing radiation, occurring in France or likely to affect French territory;

– contributing to keeping the public informed with regard to nuclear safety and radiation protection issues."

In 1976, the CEA units assigned to studies and research in radiological safety and protection (as well as security) were merged to form the Institute for Protection and Nuclear Safety (*Institut de protection et de sûreté nucléaire*, IPSN), whose first director was Jean Bourgeois, former Chairperson of SCSP (renamed the Pile Safety Commission [*Commission de sûreté des piles*, CSP]). This institute for research and assessment was responsible for providing technical support to public authorities, especially to SCSIN and later DSIN (see below).

IPSN's autonomy within CEA was reinforced on several occasions to better mark the independence it exercised when conducting assessment missions involving the development of nuclear energy, as CEA is both a nuclear operator and a research institute in this field. In 2002, at the same time the DGSNR was created, the French Institute for Radiological Protection and Nuclear Safety (*Institut de radioprotection et de sûreté nucléaire*, IRSN) was founded, bringing together the technical teams from IPSN (CEA), OPRI and the permanent secretariat of CIREA in a single, independent public agency.

IRSN's missions were defined by Decree 2002-254 of 22 February 2002 and replaced by Decree 2016-283 of 10 March 2016, which clarified existing missions and also added new ones. These texts define six main missions, which exclude any nuclear operator activity:

- conducting assessments, research and analyses, monitoring and dosimetry for public or private organizations in France and other countries;
- defining research programmes, carried out within IRSN or entrusted to other French or foreign research organizations, with a view to maintaining and developing the skills required to perform assessments in its areas of specialization; this essential mission for maintaining IRSN's assessment capability will be illustrated in Chapter 39;
- contributing to providing radiation protection training to health sector professionals and workers subject to exposure;
- providing technical support to public authorities and safety authorities, including in the event of an incident or accident involving ionizing radiation sources, by proposing technical, health and medical measures to ensure the protection of the public, workers and the environment and to restore a safe state in the affected facilities;
- maintaining continuous oversight of radiation protection, in particular by contributing to environmental radiological monitoring, managing and analysing dosimetry data pertaining to personnel exposed to ionizing radiation and managing the inventory of ionizing radiation sources;
- contributing to keeping the public informed.

The Act passed on 13 June 2006 on Nuclear Transparency and Security (TSN Act) marked an important milestone in the development of regulatory control of nuclear facilities, creating an independent administrative authority responsible, on behalf of the State, for regulating and controlling nuclear safety and radiation protection to protect the public, patients, workers and the environment. It is also responsible for keeping citizens informed on nuclear safety issues. This entity is the French Nuclear Safety Authority (*Autorité de sûreté nucléaire*, ASN), whose missions and organization are described in Section 2.3.

The TSN Act also specifies the role, missions and operating procedures of the local information commissions (*Commissions locales d'information,* CLIs), set up beginning in 1981 at sites with one or more basic nuclear installations. The commissions have joined together to form an association called the French National Association of Local Information Committees and Commissions (*Association nationale des comités et commissions locales d'information*, ANCCLI). There are about thirty local information commissions that cover civilian basic nuclear installation sites[21].

[21] The committees focus on basic nuclear installations that are of interest with regard to national defence issues.

The TSN Act also created a High Committee for Transparency and Information on Nuclear Security (*Haut comité pour la transparence et l'information sur la sécurité nucléaire*, HCTISN[22]), an interdisciplinary body for information, consultation and discussion of the risks associated with nuclear activities and the impact of these activities on people, the environment and nuclear security. Composed of members[23] appointed for six years by decree, it may issue an opinion on any matter in these areas, including inspections and related information. Its opinions are made public.

Finally, the French Parliamentary Office for Evaluation of Scientific and Technological Options (*Office parlementaire d'évaluation des choix scientifiques et technologiques*, OPECST), described below, plays a role in nuclear safety by organizing hearings and preparing general and specific reports on nuclear safety and radiation protection issues.

Facilities and activities related to national defence are organized separately, operating under a specific safety authority, and therefore are not covered in this book.

The remainder of this chapter will primarily concern the concepts, principles and regulations applicable to pressurized water reactors in French nuclear power plants.

2.2. A few definitions

Before going any further, a few definitions have been provided as given in French regulations.

a. Nuclear security

Article L.591-1 of the French Environment Code (which incorporates the provisions of the TSN Act) defines nuclear security as follows: "Nuclear security encompasses nuclear safety, radiation protection, prevention of and protection from malicious acts, as well as civil protection in the event of an accident."

[22] See www.hctisn.fr (in French).

[23] Members include:

1. Two members from the National Assembly and two members from the Senate, with each member appointed from the ranks of these two bodies, respectively;
2. Representatives of local information commissions (CLIs);
3. Representatives of environmental non-profit organizations and other non-profit organizations mentioned in Article L.1114-1 of the French Public Health Code;
4. Representatives of people responsible for nuclear activities;
5. Representatives of the relevant employee trade unions;
6. People recognized for their competence in dealing with scientific, technical, economic or social issues, or for their skills in information and communication, including three designated by the French Parliamentary Office for the Evaluation of Scientific and Technological Options, one by the French Academy of Sciences and one by the French Academy of Moral and Political Sciences;
7. Representatives from ASN, relevant government services and IRSN.

French regulations are therefore based on a broader definition of nuclear security than that commonly used internationally, namely in the IAEA glossary. According to the IAEA, 'nuclear security' covers the entire range of measures devised to prevent, detect and respond to theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, any other radioactive substances and facilities containing these materials. In this sense, international nuclear security therefore aims to ensure protection against actions of malicious origin, a concept that covers both the theft or diversion of nuclear materials as well as acts of sabotage that could lead to radiological consequences for people and the environment.

b. Nuclear safety

Nuclear safety, a subset of nuclear security, is defined by French regulations as "the set of technical provisions and organizational measures relative to the design, build, operation, shutdown and decommissioning of basic nuclear installations, and the transport of radioactive substances that are taken to prevent and mitigate accidents."

Nuclear safety therefore involves preventing the risk of radiological or non-radiological accidents related to the operation of basic nuclear installations and mitigating accidents that may occur despite the preventive measures implemented.

c. Radiation protection

Radiation protection is another subset of nuclear security, defined as "all the rules, procedures and means of prevention and monitoring implemented to stop or mitigate the direct or indirect harmful effects of ionizing radiation on human health, including through environmental impact." Radiation protection rules that apply to the public are defined in the French Public Health Code, while those specific to workers are defined in the Labour Code.

d. 'Protected interests'

The TSN Act aimed to bring the regulatory regime applicable to basic nuclear installations as close as possible to the more general regulatory regime applicable to hazardous facilities, known as 'Installations Classified for Environmental Protection', while including a number of specific features for basic nuclear installations.

In particular, Article L.593-7 of the French Environment Code, in which the TSN Act was enacted, provides that a construction authorization for a basic nuclear installation can be issued only if, "taking into account current scientific and technical knowledge, the operator demonstrates that the technical and organizational measures taken or envisaged [...] are capable of preventing or sufficiently mitigating the risks and detrimental effects that the facility presents for [public security, health, and hygiene and the protection of nature and the environment – grouped under the notion of 'protected interests']" (this authorization is issued by decree, based on a report from the ministers responsible for nuclear safety).

The TSN Act therefore requires that detrimental effects associated with normal operation, such as noise pollution and any impact on fauna and flora, be addressed in the context of the construction authorization and subsequent approvals. It led to extending the historical concept of 'item important to safety'[24], in force since the Quality Order of 10 August 1984, to include the notion of 'item important to protection' during preparation of the Order of 7 February 2012, which laid down the general rules applicable to basic nuclear installations (INB Order), and repealed the Order of 10 August 1984.

2.3. The different contributors to nuclear safety and their missions

Since the creation of the French Institute for Radiological Protection and Nuclear Safety (IRSN) as a State public body in the early 2000s and enactment of the TSN Act in 2006, nuclear safety issues at basic nuclear installations have involved:

- public authorities, particularly ASN,
- facility operators,
- assessment organizations[25],
- civil society.

Research work is conducted by facility operators, organizations providing assistance to designers and operators (such as CEA) and assessment organizations.

a. Public authorities

Parliament intervenes in nuclear safety and radiation protection issues by passing laws, such as Act 2006-686 of 13 June 2006, known as the TSN Act, and the Act of 28 June 2006 on sustainable management of radioactive materials and waste.

The French Parliament's interventions are supported by the Parliamentary Office for Evaluation of Scientific and Technological Options (*Office parlementaire d'évaluation des choix scientifiques et technologiques*, OPECST) created by Act 83-609 of 8 July 1983, comprising 18 members from the National Assembly and the Senate, appointed in proportions representative of the elected political parties, and constitutes a

[24] The operator of a basic nuclear installation must ensure that the quality achieved in the design, build and maintenance of the facility structures, equipment, materials, interconnecting assemblies and operating conditions is commensurate with the importance of the corresponding safety functions. For this purpose, the operator must ensure that a system is implemented to define the quality of the above elements, to obtain and maintain that quality, to check that it is obtained and maintained, and to analyse and correct any deviations. This system is applied from the design phase and extends throughout all subsequent phases of the lifetime of the basic nuclear installation. This subject will be covered in further detail in Section 7.4.

[25] IRSN is usually the main contact, although ASN has occasionally sought advice from other organizations, such as INERIS, on specific topics.

common source of information for the National Assembly and the Senate. The mission of OPECST is "to inform Parliament of the consequences of scientific and technological choices so that it can make informed decisions." To fulfil its mission, OPECST "collects information, implements study programmes and conducts assessments." For example, OPECST has issued reports on nuclear activities involving topics such as State control of nuclear facility safety and radiation protection, long-term management of radioactive waste, the operating lifetime of nuclear power plants and the development of new types of reactors. OPECST regularly holds hearings with ASN, IRSN and operators on subjects under investigation; some hearings involve non-profit organizations (such as Greenpeace or others).

In the field of nuclear safety, the government formulates general regulations in application of the TSN Act by passing decrees and orders, issuing construction authorizations, passing decrees for final shutdown and 'prescribing' decommissioning of basic nuclear installations. The Nuclear Safety and Radiation Protection Mission (*Mission de la sûreté nucléaire et de la radioprotection*, MSNR) was set up for this purpose within the Directorate-General for Risk Prevention (*Direction générale de la prévention des risques*, DGPR) of the Ministry for Ecological and Inclusive Transition.

In application of the TSN Act, regulatory decisions of a technical nature as well as certain individual decisions taken by ASN[26] can only come into force once they have been approved by the ministers responsible for nuclear safety. Approval takes the form of a ministerial order.

ASN, created by the TSN Act, is an independent administrative authority which, on behalf of the State, conducts missions to control nuclear safety and radiation protection (for workers, the environment and the general public), and keeps the public informed on these issues. Its missions include the following:

1. ASN **contributes to the preparation of regulations** by giving its opinion on draft versions of decrees and ministerial orders within its areas of competence and by taking the technical regulatory decisions required to enact these decrees and orders;

2. ASN **authorizes commissioning of basic nuclear installations** and checks compliance with the rules and regulations applicable to basic nuclear installations, often by conducting on-site inspections;

3. ASN **is involved in managing radiological emergency response operations**: it makes recommendations to the competent regulatory authorities (government, prefects, etc.) on medical and health measures, as well as civil security;

4. ASN **participates in keeping the public informed**, including during emergency situations.

ASN is led by a Commission formed by five commissioners, appointed for a non-renewable six-year term, three of whom (including the Commission Chairperson) are

[26] This includes decisions on discharge limits for basic nuclear installations.

appointed by the President of the French Republic, the fourth by the President of the National Assembly, and the fifth by the President of the Senate. ASN departments operate under the authority of the ASN Chairperson.

The ASN's Director General is appointed by the Chairperson. He or she organises ASN's activities within various departments. The departments manage the various areas of ASN's activity at the national level, including granting authorizations for facility construction and commissioning, performing periodic reviews, approving transport packaging, etc. and participate in establishing general regulations and ASN decisions. At the national level, the departments coordinate the regional offices[27], which conduct most on-site inspections and review 'routine' requests (such as temporary exemptions from operational limits and conditions) concerning nuclear activities in their region.

ASN's Nuclear Pressure Equipment Department (*Direction des équipements sous pression nucléaires*, DEP) deserves special attention. Formerly known as the French Inspectorate of Nuclear Steam Supply Systems (*Bureau de contrôle des chaudières nucléaires*, BCCN), then as the Nuclear Construction Inspection Agency (*Bureau de contrôle de la construction nucléaire*), this department, based in Dijon, is responsible[28] for inspecting pressure equipment in basic nuclear installations, especially the reactors in the nuclear power plant fleet. It also participates in drafting regulations on pressure equipment. The Focus feature at the end of this chapter provides some historical background on the regulation of pressure equipment as applied in the nuclear field, as well as the early history and roles of BCCN and then DEP.

In accordance with the TSN Act, ASN issues an annual report that is submitted to the government, the President of the French Republic and Parliament – where it is referred to OPECST. At the request of the relevant committees of the National Assembly, the Senate or OPECST, the ASN Chairperson reports on the authority's activities.

[27] ASN's eleven regional offices (in 2019), with jurisdiction over one or more administrative regions, operate under the authority of regional representatives designated by the ASN Chairperson. These divisions are based in eleven cities in France: Bordeaux, Caen, Châlons-en-Champagne, Dijon, Lille, Lyon, Marseille, Nantes, Orléans, Paris and Strasbourg.

[28] It should be noted that, until 2006, the Regional Industry, Research and Environment Directorates (*Directions régionales de l'industrie, de la recherche et de l'environnement*, DRIRE) carried out a certain number of missions in the field of nuclear safety and radiation protection. Since then, these missions have come under the responsibility of ASN and its regional offices. The DRIRE regional directorates have been replaced by the Regional Environment and Housing Directorates (*Directions régionales de l'environnement et du logement*, DREAL and DRIEE for the Paris region), which continue to be in charge of inspection and safety of industrial activities, energy production and energy control (excluding nuclear power), with a particular focus on non-nuclear pressure equipment.

With regard to public information, in the aftermath of the Chernobyl accident, SCSIN created the *Bulletin sur la sûreté nucléaire* (Nuclear Safety Bulletin), which was renamed *Contrôle Review*[29] in 1994.

In an effort to enhance transparency and keep the public informed, ASN now consults stakeholders when preparing regulatory and individual decisions with an environmental impact, or guides and certain other texts in their draft version. In this way, since its creation in 2006, ASN has been able to collect comments from the public on the draft version of its general regulatory decisions regarding nuclear safety and radiation protection.

Following the same approach, ASN decided to allow representatives of civil society to participate in advisory committees (standing groups of experts) (see below under Subsection d).

On its website, ASN releases information on significant events reported by facility operators, along with a certain number of decisions, opinions, reports, 'educational files' and 'information sheets', including opinions issued by the advisory committees (see below). It also includes announcements about various public consultations and draft regulations submitted for public review.

Finally, it may be useful to mention three other entities (not an exhaustive list) involved in nuclear security issues:

– the Environmental Authority, who releases opinions on environmental issues when reviewing applications for authorizations to build civilian basic nuclear installations;

– the Senior Defence and Security Official (*Haut fonctionnaire de défense et de sécurité*, HFDS) from the Ministry for Ecological and Inclusive Transition, who is responsible for implementing measures required to protect and control nuclear materials[30] in order to keep them safe from malicious acts;

– the General Secretariat for Defence and National Security (*Secrétariat général de la défense et de la sécurité nationale*, SGDSN), which reports to the Prime Minister, is in charge of emergency response at the national level. In February 2014, it issued the French National Emergency Response Plan for a Major Nuclear or Radiological Accident[31], which describes how emergency response is organized nationwide, the strategy to be applied and the various areas in which measures must be taken in the event of a major nuclear or radiological accident. The French National Emergency Response Plan for a Major Nuclear or Radiological Accident is discussed in greater detail in Chapter 38 on emergency response management.

[29] The news bulletin *Contrôle Review*, published by ASN two or three times a year, presents three features: 'Analysis', covering a technical topic or regulatory issue, 'Operating Experience Feedback', focused on a technical matter, and 'At Issue', addressing technical or societal questions.

[30] Plutonium, uranium, thorium, deuterium, tritium and lithium-6.

[31] Reference 200/SGDSN/PSE/PSN, February 2014.

b. Facility operators

As at 31 December 2017, 187 civilian basic nuclear installations were listed in ASN Decision 2018-DC-0624 dated 30 January 2018, eight of which have been decommissioned since 13 June 2006[32] (see Figure 2.1).

The operator of a basic nuclear installation is the main person responsible for facility safety (a principle stated explicitly in the French Environment Code), since at any given time, only the operator is capable of taking the concrete action required.

In France, there are four main operators of basic nuclear installations:

- Électricité de France (EDF), which operates pressurized water reactors in its nuclear power plant fleet (56[33] in service, not including the Flamanville 3 EPR, which is in the startup phase);
- Areva NC – which became Orano Cycle in 2018 – operates the main fuel cycle facilities (fuel fabrication, spent fuel treatment, reprocessing);
- the Atomic Energy and Alternative Energy Commission (*Commissariat à l'énergie atomique et aux énergies alternatives*, CEA), which mainly operates research reactors and laboratories;
- the French National Radioactive Waste Management Agency (*Agence nationale pour la gestion des déchets radioactifs*, Andra), which operates radioactive waste storage facilities.

The history and size of these operators means that they are also involved, to a greater or lesser extent, in designing their facilities, which gives them very extensive experience in safety matters. They are, of course, invited to participate in public debates conducted by ASN in the process of preparing regulations applicable to operators or guides on best practices.

In addition to these major operators, there are also smaller operators who work with systems such as particle accelerators (GANIL), irradiators (Ionisos, Synergy Health), radiopharmaceutical production plants (CIS Bio International), research facilities or those dedicated to experimentation (ITER Organization for the ITER facility at Cadarache, Institut Laue-Langevin for the high-flux reactor in Grenoble, etc.). These facilities often have specific risk characteristics that must be taken into account in the safety demonstration and during review of the safety demonstration by safety organizations.

[32] It does not include facilities no longer considered as basic nuclear installations or those decommissioned prior to 13 June 2006.

[33] Taking into account shutdown of Units 1 and 2 at the Fessenheim nuclear power plant in 2020.

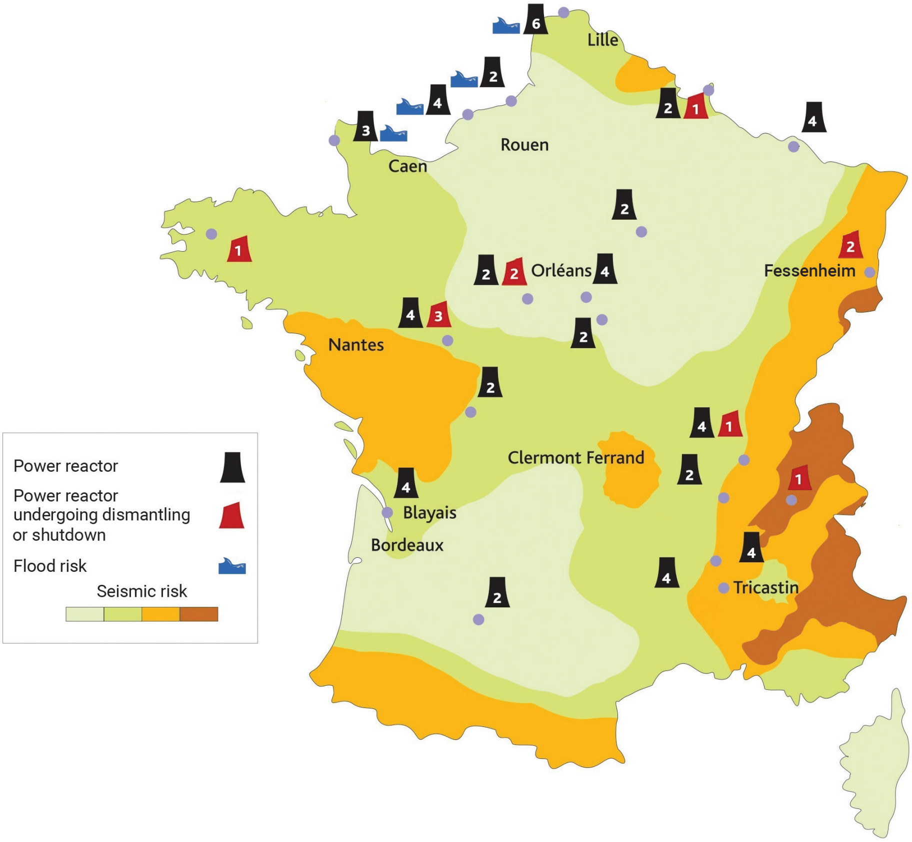


Figure 2.1. Location of NPP-type basic nuclear installations in France (including gas cooled reactors and sodium fast-neutron reactor SUPERPHENIX, undergoing dismantling). IRSN.

The TSN Act also requires that nuclear facility operators provide information on any event that may occur within their facilities: "All operators of basic nuclear installations shall prepare an annual report covering:

- nuclear safety and radiological protection measures taken;
- nuclear safety and radiological protection incidents and accidents that must be officially reported [...] when they occur on the premises of the facility, as well as the preventive and mitigation measures taken to limit their impact on human health and the environment;
- monitoring systems and the resulting data pertaining to radioactive and non-radioactive discharges released from the facility into the environment;
- the nature and quantity of radioactive waste stored at the facility, and measures taken to limit the volume and effects of waste on human health and the environment, especially in soil and water."

This report is made public and copies are sent to the local information commission and the High Committee for Transparency and Information on Nuclear Security (HCTISN).

A noteworthy commitment was made by the nuclear power plant operator, EDF, in its document *Nuclear Safety Policy of the EDF Group*, issued on 20 January 2012: "Dialogue and transparency are essential to gain everyone's trust by providing clear and faithful information on events and their possible impact; the aim is to provide and maintain good communication with employees and their representatives, subcontractors, regulatory authorities, local communities and all other nuclear safety stakeholders."

c. IRSN: the assessment and research organization

Within the French system for controlling nuclear facilities, IRSN is recognized as a state-owned industrial and commercial enterprise (EPIC), specified by Decree 2002-254 of 22 February 2002 and updated by Decree 2016-283 of 10 March 2016. IRSN reports to five supervisory ministries (Ecology, Research, Energy, Health and Defence). It is the primary institutional expert in nuclear and radiological risks, providing support to public authorities, especially for basic nuclear installations. It assesses exposure of people and the environment to ionizing radiation and proposes measures to protect the public, workers and the environment in the event of an accident. It contributes to defining public policy in its areas of activity, as was the case in 2014-2015, for example, during preparation of the act on energy transition for green growth (Act 2015-992 of 17 August 2015, known as the TECV Act).

IRSN conducts assessments, studies and research. It has a staff of approximately 1700 people working at about ten sites, including 1200 researchers and experts, both generalists and specialists (in criticality, neutron physics, mechanics, thermal hydraulics, statistics and probability, fire protection, earth sciences, medicine, biology, agronomy, metrology and others).

Since nuclear safety expertise is based on scientific and technical knowledge, IRSN aims to ensure a continuously high level of expertise by devoting significant resources to:

- monitoring and learning lessons from incidents and accidents both in France and in other countries,
- studies and research.

At the request of ASN, IRSN reviews safety cases submitted by operators of basic nuclear installations (to authorize facility construction, commissioning, changes, periodic review or dismantling, for example), which must include the appropriate support documentation, commonly referred to as the 'safety demonstration', and submits its opinions and recommendations. IRSN's assessment provides decision-making support based on the best available scientific and technical knowledge.

The safety demonstration[34] consists of documents written by the operator, who must substantiate the safety of the facility under its responsibility and commit to meeting the conditions provided in these documents. Once IRSN has reviewed the justifications presented in these documents, it sends a written opinion, accompanied by the necessary explanations regarding the results of its assessment, to ASN, which then takes any appropriate action.

It should be emphasized that assessment is not just a question of ensuring compliance with regulations. While the role of IRSN is defined in a regulatory context that must be taken into account, it aims to provide technical insight based on current knowledge and in-depth analysis. This requires, on one hand, the availability of extensive and up-to-date knowledge in the various scientific and technical areas concerned and the ability to draw conclusions through various approaches, and, on the other hand, continuous technical dialogue, on equal footing with operators.

High-quality technical exchanges with operators, where each party assumes its own responsibilities, are essential to properly assess the proposals contained in cases under review and to ascertain whether there are realistic possibilities for improving safety. In this way, the Institute and operators mutually share their concern for safety.

As the studies and research in which IRSN is involved require significant resources, they are most often conducted in collaboration with other partners (usually CEA), in various frameworks (national, European, international), and may also involve universities or the French National Centre for Scientific Research (*Centre national de la recherche scientifique*, CNRS). A few of the major topics covered in studies and research on the safety of pressurized water reactors include the following:

- the behaviour of the fuel in degraded situations and the resulting transfers of radioactive substances (incidents, accidents, including the case of fuel melt or core melt);
- phenomena that may occur in a core-melt accident (such as a steam explosion, hydrogen explosion or molten corium-concrete interaction);
- various phenomena arising in the event of fire, etc.

The knowledge (data, models, etc.) resulting from these studies and research is most often integrated into simulation software used to conduct studies, such as ASTEC for simulating core-melt accidents.

It should also be noted that in terms of studies, since the 1980s IRSN has developed its own models for probabilistic safety assessments (PSAs, covered in Chapter 14) for reactors in the French nuclear power plant fleet, to gain acute knowledge on

[34] In *Analyse de sûreté des installations nucléaires – Principes et pratique* (Nuclear Facility Safety Analyses – Principles and Practices), *Techniques de l'ingénieur* BN3810 V1, 10 July 2017, D. Quéniart notes that this is “a somewhat misleading expression in that it evokes a form of infallibility that experience refutes on a regular basis.”

reactor operation and discuss lessons learned with the operator, EDF, comparing the PSA models used by both parties.

There are three entities that advise IRSN and assess its research, including prominent French and foreign scientists:

- the Nuclear Safety and Radiation Protection Research Policy Committee[35], headed by the Chairperson of IRSN's Board of Directors and composed of representatives of public authorities, businesses and professional associations, employees from the nuclear sector, elected officials, non-profit organizations, research organizations and qualified leading figures from France or other countries;
- the Scientific Council, whose members (largely from academia) are designated by the supervisory ministries, headed by a leading figure from the scientific world;
- the Inspection Committee[36], composed of experts appointed by IRSN's Director General, where about half of the members are from foreign organizations[37].

The Research Policy Committee and Scientific Council direct IRSN's research work by setting objectives and priorities (through the Policy Committee), and achieving these objectives through IRSN's programmes (guided by the Scientific Council).

The Inspection Committee evaluates IRSN's scientific and technical activities based on their achievements, with a particular focus on the scientific quality of the research conducted and the results. To this end, work conducted by the Inspection Committee is performed in cooperation with the external assessment entity of IRSN[38], approved by HCERES[39].

IRSN's international dimension in the field of nuclear safety is seen in the cooperation agreements signed with more than forty countries and its contribution to the creation and coordination of the European Technical Safety Organisations Network (ETSON), discussed in Chapter 3[40].

[35] This Committee (*Comité d'orientation des recherches en sûreté nucléaire et en radioprotection*) was established in 2008. Decree 2016-283 of 10 March 2016, founding the Institute for Radiological Protection and Nuclear Safety, made this committee official, specifying its composition and procedures for appointing its members.

[36] A committee formed by IRSN, not provided for in the decree of 10 September 2016.

[37] This measure is applied to avoid conflicts of interest.

[38] This entity is composed of the members of the Inspection Committee and external experts selected according to the subject matter being assessed.

[39] Created by Act 2013-660 of 22 July 2013 on higher education and research, the High Council for the Evaluation of Research and Higher Education (*Haut conseil de l'évaluation de la recherche et de l'enseignement supérieur*, HCERES) replaced the Agency for the Evaluation of Research and Higher Education (*Agence d'évaluation de la recherche et de l'enseignement supérieur*, AERES).

[40] For a fuller understanding of IRSN's international cooperation work, see J. Couturier and M. Schwarz, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2018.

With regard to scientific and technical information for the general public, IPSN, in its early days, made a contribution by publishing educational works to be used not only by professionals, but also a relatively knowledgeable public.

However, Decree 2016-283 of 10 March 2016, issued in application of the Energy Transition Act of 17 August 2015 (TECV Act), emphasized the importance of IRSN's mission of communicating with the public; the decree stipulates that "the Institute for Radiological Protection and Nuclear Safety contributes to transparency and keeping the public informed on nuclear safety and radiation protection, especially by preparing and publishing an annual activity report. This report is submitted to the relevant supervisory ministers and is presented to the High Committee for Transparency and Information on Nuclear Security, the High Council of Public Health and the Working Conditions Orientation Council." In accordance with the provisions of Article L.592-47 of the French Environment Code, IRSN "shall publish its opinions, when they do not involve national defence, at the request of a public authority or the French Nuclear Safety Authority (ASN), in conjunction with the relevant authority."

Since its foundation in 2002, IRSN has implemented a policy of 'opening up to civil society' on nuclear safety and radiation protection issues (involving people and the environment) by responding, for example, to requests from local information commissions (CLIs) and by participating in interdisciplinary expert assessment groups[41] and joint programmes led with several partners[42]. In 2003, IRSN and ANCCLI (presented later in Subsection e) signed a cooperation agreement committing IRSN to provide scientific and technical support to CLIs in the areas of nuclear safety and radiation protection. In addition, IRSN regularly publishes various nuclear safety assessment reports on its website. In this context, from 2008 to 2017 IRSN published its point of view on the state of the nuclear power plant fleet for each year of operation, highlighting a few key points in terms of safety and radiation protection.

It should be noted that, since 2014, discussions[43] with civil society have been pursued on a certain number of subjects involved in periodic review associated to the fourth ten-yearly inspection outages of 900 MWe reactors (for example, the ageing of reactor

[41] An example is the Nord-Cotentin Radioecology Group (*Groupe radioécologie Nord-Cotentin*, GRNC), founded in 1997 in a context of controversy following the publication of an epidemiological study by Professor Jean-François Viel on the incidence of leukaemia in the Beaumont-La Hague area, i.e. in an environment close to irradiated-fuel processing plants.

[42] IRSN has been involved in a number of safety and radiation protection matters, including:
- the Loire Environmental Pilot Project (*Action pilote environnement Loire*, APEL), launched in 2005 with the local information commissions of the Loire basin (mainly those of Dampierre-en-Burly and Saint-Laurent-des-Eaux), which led to the publication of the first joint report by IRSN and these CLIs in late 2008;
- the Interdisciplinary Approach to Air Quality and Radon Risk in Burgogne-Franche-Comté, launched in 2011, which aims to assist the inhabitants of this region in managing the risk associated with radon and to integrate the management of this risk into home energy renovation projects.

[43] Involving ASN, IRSN and ANCCLI.

vessels and containment structures), entailed by EDF's request to continue the operation of these reactors beyond 40 years (the 'Operating Lifetime' project[44]) – see Section 3.2.

d. Advisory Committees

For certain important technical issues on safety and radiation protection – such as (from a nuclear safety prospective) licensing, commissioning and periodic review of basic nuclear installations, or certain draft regulations or quasi-statutory regulations – ASN may need to consult advisory committees[45], which first came into existence in 1972. ASN has created seven advisory committees (*Groupes permanents d'experts*, GPE), each with its own area of expertise (reactors [GPR], transport of radioactive and fissile materials [GPT], laboratories and plants [GPU], radiation protection (industry, research) and the environment [GPRAD], radiation protection for healthcare professionals, patients and the public for medical or forensic applications of ionizing radiation [GPMED], waste [GPD], and nuclear pressure equipment [GPESPN]). An advisory committee on decommissioning was created in 2018 (GPDEM).

The advisory committees are composed of members appointed by ASN in a personal capacity, based on their competence, according to a procedure that aims to achieve an appropriate diversity of expertise while limiting any risk of a conflict of interest given the subjects to be covered. Committee members come from universities and non-profit organizations as well as French and foreign research and assessment organizations, including IRSN, but may also come from operational facilities. They may be currently employed or retired. Since June 2014, the pluralism of these committees has been enhanced by nominating members from civil society (such as members of local information commissions and non-governmental organizations). For a given topic, each advisory committee can also seek assistance from recognized specialists in specific fields (from France or other countries).

The advisory committees dealing with nuclear safety issues generally discuss cases submitted by an operator and the assessment of this operator by IRSN, or ASN/DEP in the case of issues concerning nuclear pressure equipment. They formalize their conclusions in opinions and recommendations addressed to ASN. The opinions and recommendations of advisory committees are made public.

For pressurized water reactors in the nuclear power plant fleet, the two most consulted advisory committees are certainly:

- the Advisory Committee for Reactors (GPR),
- the Advisory Committee for Nuclear Pressure Equipment (GPESPN).

[44] This project is described and discussed in Section 30.5.

[45] Similar groups exist, such as the Advisory Committee on Reactor Safeguards (ACRS), which works in the USA with the NRC, and the Reactor Safety Commission (*Reaktorsicherheits-kommission*, RSK) in Germany.

e. The public and civil society: from information to involvement

In addition to legislation and regulatory bodies, the history of nuclear safety control would not be complete without taking a brief look at the gradual involvement of civil society[46].

Decree 73-278 of 13 March 1973 created the Central Service for the Safety of Nuclear Installations (SCSIN) as well as the High Council for Nuclear Safety (*Conseil supérieur de la sûreté nucléaire*, CSSN). CSSN's mission covered all technical issues concerning the safety of nuclear facilities falling within the remit of the Minister for Industry. It was tasked with assessing the overall results of activities pursued in this area, especially those conducted by SCSIN. While its members included a significant proportion of institutional representatives, it also included five leading figures specialized in the required subject matters[47].

A decree of 10 November 1977 created the Nuclear Energy Information Council (*Conseil de l'information sur l'énergie électronucléaire*, CIEE), placed under the authority of the Prime Minister, with CSSN maintaining its technical role. CIEE's mission was to ensure that the public had access to technical, health, environmental, economic and financial information on nuclear energy. In addition to leading figures in various fields (energy, economics, communication techniques, etc.), it included[48] six representatives of environmental non-profit organizations. CIEE issued annual reports on various topics (such as the health effects of radioactivity and what becomes of facilities and waste) and worked to ensure that SCPRI reports were made public.

In 1979, however, when the accident at the Three Mile Island nuclear power plant occurred, extensive feedback was made in France. It was during this time that a decree dated 29 October 1981 modified the composition of the CSSN, in particular to include three representatives of environmental non-profit organizations. Consequently, the CIEE was dissolved.

The 1986 accident at the Chernobyl nuclear power plant was marked in France by issues in communicating with the public. This led to another reorganization of the CSSN by a decree of 2 March 1987: the CSSN became the High Council for Nuclear Safety and Information (*Conseil supérieur de la sûreté et de l'information nucléaires*, CSSIN), comprising six people specialized in reporting and communication. The journalist Pierre Desgraupes was appointed Vice Chairman, alongside the High Commissioner for Atomic Energy, the other Vice Chairman. Pierre Desgraupes pushed to create a nuclear incident severity scale, implemented in 1988, to give the public a better understanding of the relative importance of different types of incidents. This scale prefigured the INES scale adopted later by the IAEA and implemented in the early 1990s (see Section 34.10).

[46] The work of P. Saint Raymond cited above, particularly chapters 9 and 11, provided significant material for this section.

[47] Its first president was Louis Néel, winner of the Nobel Prize in Physics.

[48] It was chaired by Simone Veil, Minister of Health and Social Security at the time.

Moreover, the way the Chernobyl accident was managed in France in 1986 generated lasting suspicion and mistrust on the part of the public towards the authorities and public institutions, leading to the creation of assessment organizations such as the Association for the Control of Radioactivity in the West (*Association pour le contrôle de la radioactivité dans l'Ouest*, ACRO) and the Commission for Independent Research and Information on Radioactivity (*Commission de recherche et d'information indépendantes sur la radioactivité*, CRIIRAD).

Under the TSN Act of 2006, mentioned above, the CSSIN was replaced by the High Committee for Transparency and Information on Nuclear Security (HCTISN).

In terms of actual involvement, although civil society has only recently been recognized as a component of the nuclear safety and radiation protection control system, and even though it was active previously[49], it now plays a much more significant role.

Even before the accidents at Three Mile Island (1979) and Chernobyl (1986), the 1970s had marked a turning point. Until then, building and operating nuclear power plants had raised few questions from the public. However, in 1974, French Prime Minister Pierre Messmer decided to launch a major nuclear power programme that called for building thirteen 900 MWe units[50] in two years. In late 1974, as part of this programme, the Minister of Industry sent the prefects a file, which was then distributed to local authorities (regional councils, etc.), on the location of the planned nuclear sites. In 1975, EDF was asked to provide environmental impact studies[51] for these sites.

Following the initiation of this programme, a group of CNRS scientists launched a petition in February 1975 entitled "Appeal by Scientists Regarding the French Nuclear Programme", which was intended as a warning regarding the dangers associated with the nuclear industry, pointing out that a nuclear accident and radioactive leaks were possible and that it would also be necessary to manage the waste produced by nuclear power plants. It questioned whether energy independence could be achieved through nuclear power, given France's limited uranium resources. It also called into question the nuclear safety control system in France and demanded a 'real debate' on nuclear energy. The petition was signed by more than 400 scientists in one week, reaching over 4000 in three months.

This action led to the creation of associations such as the Group of Scientists for Information on Nuclear Energy (*Groupement de scientifiques pour l'information sur*

[49] The public was already involved in public inquiries conducted in connection with reviews for various construction authorizations and decommissioning applications for basic nuclear installations.

[50] Reactors have been implemented in 'plant units' under successive 'programme contracts' (except for the initial reactors at Fessenheim and Bugey, which only came under a 'programme contract', designated 'CP0', after the plants had been built). The term 'unit' is therefore commonly used instead of 'reactor' in nuclear engineering and safety in France.

[51] This was in anticipation of Act 76-629 of 10 July 1976, making it mandatory to conduct an impact assessment for this type of project.

l'énergie nucléaire, GSIEN), created in late 1975 by a few of the same scientists that had initiated the February 1975 petition.

At the same time, in November 1975, the nuclear branch of the CFDT trade union published an initial work, *L'électronucléaire en France* (Nuclear Power in France), which was updated and expanded in 1980 and renamed *Le dossier électronucléaire* (The Nuclear Power Case[52]).

In July 1977, the demonstration held by protesters near the Creys-Malville site, where a fast-neutron sodium cooled reactor (SUPERPHENIX) was under construction, was an important moment in the controversy[53], as was the power plant planned for the Plogoff site in Brittany, abandoned three years later.

The role of civil society has developed gradually. To respond to the concerns of the population living near the Fessenheim nuclear power plant and given the growing anti-nuclear movement, particularly in Germany and Switzerland, in 1977 the local government authority (*Conseil général*) of the Upper Rhine area set up an Oversight Commission, which included elected officials and non-profit organization representatives, to regularly review plant operations and incidents at this facility. Other commissions of this type were set up, such as the Permanent Special Commission for Information (*Commission spéciale permanente d'information*, CSPI) near the La Hague facility[54] in 1981 (replaced, in 2004, by the Local Information Commission near the Orano facility in La Hague).

Public authorities recognized the expansion of these actions when a circular was signed by Prime Minister Pierre Mauroy on 15 December 1981. This circular invited local government authorities (*Conseils généraux*) to set up a local information commission (CLI) for each major industrial facility in the country, belonging to the energy supply chain[55]. Some thirty CLIs have been created since then.

A Local Information and Monitoring Commission for the Bure Underground Laboratory (Bure CLIS) was likewise created in application of the Act of 30 December 1991 relating to research on radioactive waste management[56]. Information commissions for regulated nuclear defence facilities (*Installations nucléaires de base secrètes*, INBS) were also created by the Decree of 5 July 2001 pertaining to nuclear safety and radiation protection in defence nuclear facilities and activities.

At the initiative of a few chairpersons from local information commissions, the National Association of Local Information Commissions (*Association nationale des commissions locales d'information*, ANCLI) was created on 5 September 2000.

[52] CFDT (*Confédération française démocratique du travail*), *Le dossier électronucléaire*, Paris, *Le Seuil*, 1980.

[53] With, regrettably, one death.

[54] Creation of Cogéma, later merged with Areva-NC, and more recently Orano Cycle.

[55] This circular specifies that "the infrastructure covered includes thermal, conventional or nuclear power plants operating at a capacity of more than 1000 MW, irradiated fuel reprocessing plants, large-scale hydroelectric facilities and underground gas storage facilities."

[56] Act 91-1381 of 30 December 1991, relating to research on radioactive waste management.

It became the National Association of Local Information Committees and Commissions (*Association nationale des comités et commissions locales d'information*, ANCCLI) in 2006, in accordance with provisions of the TSN Act[57], for the purpose of forming a network to exchange information between CLIs and serving as a resource centre and contact point with public authorities, as well as national and international organizations in the nuclear field.

Under the terms of a 2019 decree[58], local information commissions currently bring together elected officials (from local and regional elective bodies), representatives of environmental non-profit organizations, designated members of representative trade unions, people appointed on the basis of their expertise in the nuclear field (economic stakeholders and professional unions), and, if the facility is located on an international border, an elected regional representative, a non-profit organization representative and a qualified specialist from each foreign country that lies on this border. A local information commission must be created, decided by the head of the local government authority (*Conseil départemental*)[59], once a construction authorization application has been filed for a basic nuclear installation. The general mission of the local information commission is to oversee, provide information and organize consultation on all activities pertaining to the facility.

Moreover, ASN representatives, other relevant government services and the regional health agency, as well as operator representatives, may also attend local information committee meetings in an advisory capacity and have access to the committee's work.

To keep the public informed on nuclear safety issues, the TSN Act established a certain number of principles. While the State is responsible for informing the public on the procedures and results of nuclear safety and radiation protection monitoring, everyone "has the right to obtain from the basic nuclear installation operator [...] the information in its possession, whether received or established by the operator, regarding risks related to exposure to ionizing radiation that may result from the facility's activity and the safety and radiation protection measures taken to prevent or

[57] TSN Act, Title III, Chapter II, Article 22, paragraph VII ("Local information committees may form a federation, in the form of an association, to represent them before national and European authorities and to assist the committees in matters of common interest. The resources of this federation are to be provided mainly from subsidies paid by the State and from contributions made by the member commissions." Governed by the Non-Profit Organization Act of 1 July 1901, ANCCLI unites 35 CLIs and similar organizations, including 33 CLIs focused on basic nuclear installations, the Bure CLIS, and SEIVA, the organization for exchanging information at the CEA Valduc site.

[58] Decree 2019-190 of 14 March 2019, enacting the provisions applicable to basic nuclear installations, the transport of radioactive substances and transparency in nuclear matters.

[59] Article L.125-17 of the French Environment Code, in which the TSN Act was later incorporated, stipulates that "a local information commission must be created for each site that has one or more basic nuclear installations as defined in Article L.593-2" and that "this commission has a general mission to oversee, provide information and organize consultations on matters pertaining to nuclear safety, radiation protection and the impact of nuclear activities on people and the environment as regards the site facilities. It disseminates the results of its work broadly, making it available to as many people as possible."

mitigate these risks or exposure, under the conditions defined [in the French Environment Code]."

The obligations of basic nuclear installation operators with regard to informing the public are specified in the TSN Act and presented in Section 2.3 b.

The High Committee for Transparency and Information on Nuclear Safety (HCTISN) was described earlier. It should be noted that, since 2010, the High Council for the Prevention of Technological Risks (*Conseil supérieur de la prévention des risques technologiques*, CSPRT), which succeeded the High Council for Classified Installations, previously consulted on draft regulations relating to Installations Classified for Environmental Protection[60], is also consulted on draft versions of executive orders regarding basic nuclear installations, and even on certain draft versions of ASN decisions, at the latter's request. The CSPRT is made up of representatives from various administrations, industry, environmental non-profit organizations, trade unions and elected officials.

ASN draft decisions are also subject to public consultation.

Civil society participates in working groups such as the Steering Committee for Management of the Post-Accident Phase of a Nuclear Accident or Radiological Emergency (*Comité directeur pour la gestion de la phase post-accidentelle d'un accident nucléaire ou d'une situation d'urgence radiologique,* CODIRPA, see Chapter 38). Similarly, non-profit organizations and elected officials are involved in the process of developing the National Plan on Management of Radioactive Materials and Waste (*Plan national de gestion des matières et des déchets radioactifs*, PNGMDR[61]).

Lastly, in 1998 France signed the UNECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention). In 2008, at the initiative of ANCCLI and the European Commission, a study was launched to take stock of the practical implementation of this convention in the nuclear field in Europe[62].

Further examples of civil society involvement are given in Section 3.2, with a certain number of safety issues raised in relation to reactors in the French nuclear power plant fleet.

[60] *Installation classée pour la protection de l'environnement (ICPE)*.

[61] The PNGMDR is part of the framework set up by the Programme Act of 28 June 2006 on the sustainable management of radioactive materials and waste. Its main purpose is to establish a regular review of the management of radioactive materials and waste, identify predictable needs for storage and disposal facilities, specify the capacity and storage periods required for these facilities, and define needs in terms of studies and research.

[62] The Aarhus Convention & Nuclear (ACN) approach, which has given rise to several round tables at the European level and in several countries. In France, it was the subject of studies conducted by three working groups, which resulted in a report comprising 13 recommendations. See the final French report on the ANCCLI website (https://www.anccli.org/wp-content/uploads/2014/07/Rapport-final-ACN-France-1.pdf).

2.4. A few basic principles and notions in the field of nuclear safety

Nuclear activities are carried out in France in compliance with French regulations (the Charter for the Environment, which is based on the Constitution, and various codes [environment, public health, labour and defence codes]). These codes must comply with France's international commitments or integrate the provisions of European Council directives into French law.

Since these various measures come from different sources, there is often significant overlapping between them.

The safety of nuclear facilities and activities is based on a certain number of major principles described in detail below[63].

a. Principle of prime responsibility of the operator

As noted earlier, one of the fundamental safety principles in nuclear facilities is the prime responsibility of operators for safety throughout the lifetime of their facilities. They must take all measures required in terms of design, construction and operation of their facilities to prevent and mitigate the risks associated with possible incidents or accidents. This covers the qualification of personnel, control over changes made to facilities or their operating procedures, control over subcontracted activities and safe management of waste.

Of course, the prime responsibility of the operator is applied in association with the principle of control by the State, responsible for the protection of people and property[64], which leads to the implementation of regulations, authorization procedures, inspections, etc.

b. The principles of justification, optimization and limitation

These principles, based on the ICRP recommendations presented in Chapter 1 of this book, are included in the French Public Health Code (Article L.1333-1), which states:

[63] Note that a number of them are included in the document published by the IAEA in 2006, Safety Fundamentals No. SF-1. At the international level, general principles and recommendations on nuclear safety, radiation protection, security and non-proliferation are defined in documents (called norms or standards) issued by the International Atomic Energy Agency (IAEA), created in 1957. Other sources include the principles and recommendations defined by the International Commission on Ionizing Radiation Protection (ICRP), created in 1928 and referred to in Chapter 1, or the safety objectives and 'reference levels' drafted by the Western European Nuclear Regulators' Association (WENRA) created more recently (1999). These various organizations and their missions are described in Chapter 3.

[64] This principle is stated in the Convention on Nuclear Safety. Adopted in 1994 by the Member States of the IAEA, the Convention was approved by France on 13 September 1995 and entered into force on 24 October 1996.

– "A nuclear activity or an operation may only be undertaken or exercised if it is justified by the benefits it provides, especially in terms of health, societal questions, economics or science, when weighed against the risks inherent to exposing people to ionizing radiation."

– The application of this principle may lead to prohibiting certain activities involving radioactive substances if the corresponding benefits (see Chapter 1) appear insufficient in comparison to the health risks. For example, it was in application of this principle that France decided, in 2011, to gradually discontinue the use of fire detectors[65] containing radionuclides, as soon as it was possible to implement other sufficiently effective technologies.

– "Exposure of persons to ionizing radiation resulting from an [activity or intervention] must be kept to the lowest level that can reasonably be achieved, considering technical, economic and social factors [...]."

– "Exposure of a person to ionizing radiation resulting from one [of these activities] must not cause the sum of received doses to exceed limits set by regulations, except when the person is exposed for medical reasons or for biomedical research."

c. Principle of prevention

The French Environment Code defines a principle of taking action to prevent and remedy environmental damage, giving priority to acting at the source, using the "best available techniques at an economically acceptable cost."

d. Precautionary principle

The Constitutional Act of 1 March 2005 defines the precautionary principle in these terms: the absence of certainty, given current scientific and technical knowledge, shall not delay the adoption of environmental protection measures. It is defined in the Charter for the Environment as follows: "Where there is the possibility of severe and irreversible damage to the environment, even though this is not a certainty given the current state of scientific knowledge, public authorities shall ensure, by applying the precautionary principle in the areas under their competence, that procedures are followed to assess the risks and that provisional and proportionate measures are taken to prevent the postulated technical damage." According to this principle, the absence of certainty, given current scientific and technical knowledge, must not delay the adoption of effective and proportionate measures aimed at preventing a risk of serious and irreversible damage to the environment at an economically acceptable cost (Article L.110-1 of the Environment Code).

[65] In a period of ten years, given the large number of detectors involved.

2.5. *Statutory and quasi-statutory frameworks applicable to basic nuclear installations*

a. Regulatory Pyramid

Before going any further, in order to better understand the process of developing the statutory and quasi-statutory framework[66] applicable to basic nuclear installations in France, it is necessary to explain what is known as the Regulatory Pyramid, shown in Figure 2.2.

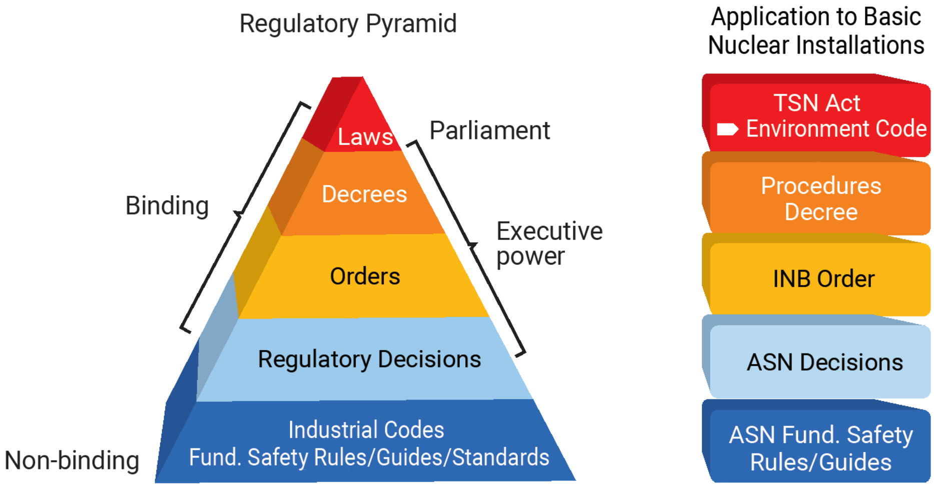


Figure 2.2. French Regulatory Pyramid. IRSN.

The texts included in this regulatory pyramid must, of course, comply with international agreements signed by France, for example, the 1957 Euratom Treaty, the 1960 Paris Convention on Third-Party Liability in the Nuclear Field, the 1994 Convention on Nuclear Safety mentioned above, and European directives, which will be discussed later. It means transposition work into French law, if necessary.

The pyramid makes a distinction between binding provisions (laws [acts], decrees, orders, regulatory decisions) and non-binding provisions, consisting of guidelines (including the fundamental safety rules established before 2006, which were followed by the ASN Guides), standards, and design or building codes established by industry that formalize proven practices, thus providing useful references that may be waived, however, if justified.

[66] Also referred to as the 'regulatory baseline'.

Directive 2009/71/EURATOM of 25 June 2009 deserves mention here. Its objectives were:

- "to establish a Community framework in order to maintain and promote the continuous improvement of nuclear safety and its regulation;
- to ensure that Member States shall provide for appropriate national arrangements for a high level of nuclear safety to protect workers and the general public against the dangers arising from ionizing radiation from nuclear installations."

This directive laid down a number of major principles to ensure control of nuclear safety:

- the existence of a regulatory authority;
- the functional separation of the regulatory authority from any other body or organization concerned with the promotion or utilization of nuclear energy; the regulatory authority shall not seek or take instructions from such bodies or organizations for the purpose of carrying out its regulatory tasks;
- the ability of the regulatory authority to carry out its tasks by employing sufficient staff with the necessary qualifications, experience and expertise; it may make use of external scientific and technical resources to support its regulatory functions;
- the ability of the regulatory authority to verify that operators (authorization holders), primarily responsible for nuclear safety in their facilities, take adequate measures to prevent accidents and mitigate their consequences; that they have the necessary financial and human resources and have the appropriate qualifications and competence;
- the existence of coercive measures used to discourage operators from committing any breach of regulations;
- providing the public with adequate information on the safety of nuclear facilities.

Directive 2014/87/EU of 8 July 2014 amended the 2009 directive following the accident at the Fukushima Daiichi nuclear power plant; it expands on the 2009 regulations with regard to periodic reviews, self-assessment of national frameworks and regulatory authorities, and international peer reviews.

In addition, the 2014 directive specifies that a regulatory authority can use external scientific and technical resources to support its regulatory functions; for instance, IRSN in France and Bel V in Belgium, which are technical safety organizations (TSOs), provide such support.

In July 2014, each Member State submitted to the European Commission a report on implementation of the directive in its 2009 version; the revised version calls for a second report by July 2020.

Finally, the 2014 directive sets a safety objective for nuclear installations that aims to limit release of radioactive substances into the environment in the event of an accident, a point that will be developed further in Chapter 18.

b. Development of the Regulatory Pyramid

From 1963 (the year of the first decree on nuclear facilities), French regulations applicable to basic nuclear installations developed gradually. For example:

- Decree 73-405 of 27 March 1973, amending Decree 63-1228 of 11 December 1963, which specifies, in particular, the procedures applicable to basic nuclear installations;
- Order of 26 February 1974 relating to the main primary system in pressurized water reactors;
- Decree 74-945 of 6 November 1974 concerning the discharge of gaseous radioactive effluent from basic nuclear installations and nuclear facilities located on the same site;
- Decree 74-1181 of 31 December 1974 on the discharge of liquid radioactive effluent from nuclear facilities;
- Decree 75-306 of 28 April 1975 relating to the protection of workers from ionizing radiation hazards in basic nuclear installations;
- Order of 10 August 1984 on the quality of the design, construction and operation of basic nuclear installations (often referred to as the 'Quality Order');
- Order of 26 November 1999 setting out the general technical requirements concerning the limits and procedures applicable to intakes and discharges performed by basic nuclear installations and subject to authorization;
- Order of 31 December 1999 setting the general technical regulations for preventing and reducing the detrimental effects and external hazards resulting from the operation of basic nuclear installations.

The limited number of documents existing at this time involved mainly procedures and did not contain detailed technical requirements. This approach was largely guided by the desire to foster an on-going technical dialogue with operators, which was facilitated by the fact that most of the operators of basic nuclear installations in France were, and still are, 'major operators'. The drawback was that French practices were not particularly clear, especially for export markets.

Therefore, from the 1980s onwards, a certain number of technical rules were developed by SCSIN and then DSIN with support from IPSN – some of which were submitted to the GPR or GPU – and published in the form of fundamental safety rules (RFS[67]). These non-binding documents were intended to specify the conditions to be met in order to comply with accepted technical practices in France. They took into account

[67] *Règles fondamentales de sûreté*.

experience acquired in the relevant subjects, particularly from review of safety analysis reports, periodic reviews, etc. Operators and designers could, nonetheless, propose different arrangements if they demonstrated that the required safety objectives were met to an equivalent degree. The list of fundamental safety rules for pressurized water reactors is given in Appendix 1.

At the same time, the French nuclear industry began to establish documents known as Design and Construction Rules (known by their French acronym RCC[68]), which formalize technical rules and principles specific to different fields, in particular for pressurized water reactors, on the basis of proven best practices (relevant to the process [RCC-P], metal structures and components [RCC-M, or RCCM-MRx for fast-neutron reactors, research reactors and nuclear fusion installations], civil works [RCC-G], fuel [RCC-C], electrical equipment [RCC-E] and fire protection [RCC-I]). The preparation and distribution of these detailed documents was not conducted under the authority of safety organizations. In the 1980s, the SCSIN officially agreed to implement certain design and construction rules through specific fundamental safety rules[69] (see Appendix 1).

c. Regulatory development since 2006

In order to be fully applicable, the TSN Act required official documents to enact these provisions. The regulations mentioned below also reinforced measures previously in effect, for example, by allowing sanctions to be applied.

The amended Decree of 2 November 2007[70], or 'Procedures Decree', thus specified certain procedures (level of authorization required, mandatory consultations, review deadlines, etc.) applicable to the construction, commissioning and operation, modification[71], decommissioning and dismantling of civilian basic nuclear installations. It also specifies the documents that must be submitted by the operator at each stage of the facility's 'lifetime' (design, construction, commissioning, modifications, decommissioning, etc.) as well as the content required in these documents (such as technical capability, financial capacity, support documents to substantiate the manner in which any risks and drawbacks of the facility are to be managed, as well as technical and organizational measures associated with operation).

[68] *Règles de conception et de construction*.

[69] Along with these rules, another document entered into effect, the SIN 3130/84 Report dated 13 June 1984, based on conclusions drawn after review of a document covering design and construction rules for PWR-based NPPs, pertaining to rules on processes for 900 MWe plant units (*Règles de conception et de construction des centrales nucléaires PWR [Recueil de règles relatives aux procédés – tranches de 900 MWe, RCC-P 900]*).

[70] Decree 2016-846 of 28 June 2016 makes significant amendments to the 2007 decree on issues involving modification of basic nuclear installations, final shutdown, decommissioning and subcontracting (use of service providers).

[71] This includes changes made to structures, systems and components and to authorized operating procedures of the basic nuclear installation.

The Order of 7 February 2012, known as the 'INB Order', defined the general rules applicable to basic nuclear installations, particularly in terms of operator organization and responsibility, with support documents demonstrating how risks, facility drawbacks, waste management and emergency situations are to be managed in a controlled manner. With the exception of a few articles, it presents a general approach, i.e. its requirements are applicable to all basic nuclear installations, from the design stage to delicensing[72]. However, "their application is based on an approach commensurate with the risks and drawbacks presented by the installation. It takes into account all relevant technical aspects, organizational factors and human factors." This leaves adequate room for technical dialogue and case-by-case assessment of facility safety.

ASN has also undertaken to develop technical regulations, prompted by the European harmonization work of WENRA, created in 1999, which revealed the very limited nature of France's technical regulations compared with those of most other European countries, even though practices in the various countries appeared to be fairly similar.

In this respect, about twenty of ASN's regulatory decisions apply or will apply the INB Order; they concern, for example, the content of safety analysis reports, periodic reviews, management of fire, flood or criticality risks, modifications to basic nuclear installations, to name a few. The establishment of non-binding guides, which may or may not constitute a supplement to regulatory decisions, has also been initiated. Their purpose is similar to that of the fundamental safety rules, which they may come to replace, under certain circumstances.

It should be noted that the INB Order repeals:

- the 'Quality Order' of 10 August 1984, cited above;
- the Order of 26 November 1999, setting out the general technical requirements concerning the limits and procedures for intakes and discharges subject to authorization, carried out by basic nuclear installations;
- the Order of 31 December 1999, setting the general technical regulations for preventing and reducing the detrimental effects and external hazards resulting from the operation of basic nuclear installations.

The list of existing statutory and quasi-statutory regulations[73] is given in Appendix 2. ASN Guide No. 22 (18 July 2017), written jointly with IRSN, is a particularly noteworthy document. This guide presents a certain number of recommendations for the design of pressurized water reactors (PWRs), with a view to preventing

[72] "Delicensing [in France] is an administrative operation that aims to permanently withdraw the facility from the list of basic nuclear installations, in which case the facility is no longer regulated under the nuclear regulatory framework and all related legal duties end as a result. This can happen only after the completion of the decommissioning works and the demonstration by the licensee that the end state has been achieved." (ASN Guide No. 6 – Final Shutdown, Decommissioning and Delicensing of Basic Nuclear Installations in France, 2016).

[73] The programme for preparing regulations is available on ASN's website using the following link https://www.asn.fr/Reglementer/Tableaux-de-suivi-INB.

radiological incidents or accidents and mitigating the consequences if they do occur[74]. The targeted public is future designers and operators of PWRs in France, but it can also be used as a reference when seeking to improve existing reactors, for example in the framework of the periodic reviews. It will be referred to extensively in Part 2 of this book, which covers the safety issues to be taken into account in designing pressurized water reactors.

The development of national technical regulations is based on a process of preparation, then consultation, involving all the entities concerned, with, lastly, a public consultation via the Internet on ASN's website (see Figure 2.3).

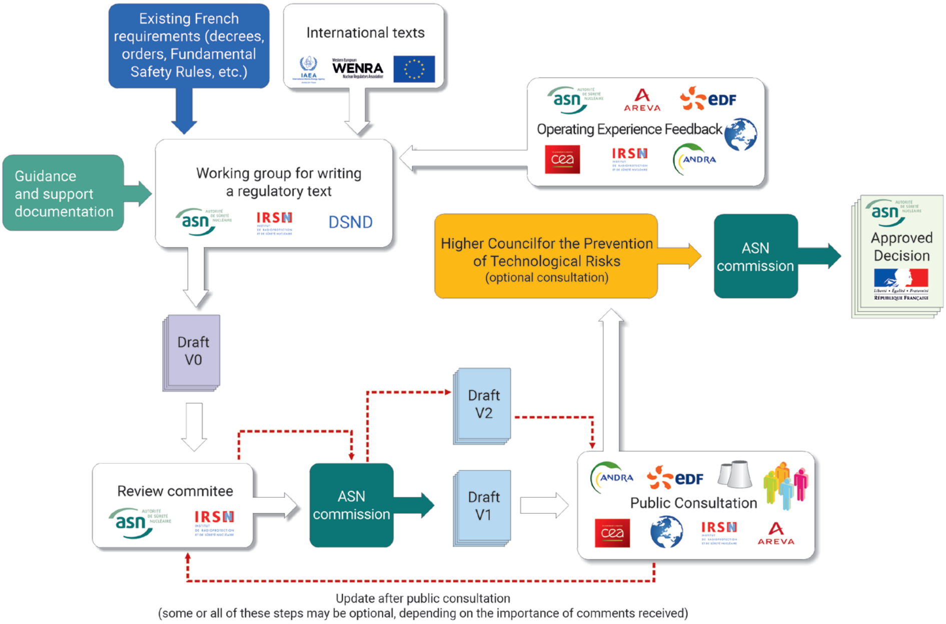

Existing French requirements (decrees, orders, Fundamental Safety Rules, etc.)
International texts
IAEA
WENRA
Operating Experience Feedback
asn
AREVA
EDF
cea
IRSN
ANDRA
Guidance and support documentation
Working group for writing a regulatory text
DSND
Higher Councilfor the Prevention of Technological Risks (optional consultation)
ASN commission
Approved Decision
Draft V0
Draft V2
Draft V1
Review commitee
ASN commission
Public Consultation
Update after public consultation
(some or all of these steps may be optional, depending on the importance of comments received)

Figure 2.3. Simplified diagram showing the main stages in the development of regulatory texts in France and the involvement of stakeholders. Georges Goué/IRSN.

[74] This guide "was written on the basis of knowledge established following technical reviews conducted on nuclear power reactors in operation, under construction or planned in France. It takes into account knowledge gained in reviewing technical cases submitted to ASN by industry, which revealed the relevance of certain practices. It will be updated regularly to take into account developments in knowledge, operating experience feedback [...], recommendations issued by international organizations and new practices."

d. The main procedures involved in operating a basic nuclear installation: from design to decommissioning

Decree 2007-1557 of 2 November 2007, as amended (most recently by Decree 2016-846 of 28 June 2016[75]), adopted pursuant to the TSN Act and the TECV Act, pertains to administrative procedures applicable to basic nuclear installations. In particular, it indicates the authorizations required for construction, commissioning, modification, final shutdown and decommissioning & dismantling of a basic nuclear installation and the documents that the operator must submit to obtain these authorizations.

The diagram shown in Appendix 3 presents the various procedures applicable to basic nuclear installations, including pressurized water nuclear reactors, and the corresponding articles of the Decree of 2 November 2007. A few points should be emphasized:

– construction or decommissioning of this type of facility is subject to a public inquiry and a decree;

– commissioning of the facility is subject to authorization by ASN;

– modifications to a basic nuclear installation that do not comply with the construction authorization delivered will require renewal of the authorization from the ministers responsible for nuclear safety (change of operator or scope of the basic nuclear installation, 'substantial' modifications);

– changes to the basic nuclear installation that do not require renewal of the authorization from the ministers responsible for nuclear safety but that are 'significant' (see Decision 2017-DC-0616 of 30 November 2017) must either be authorized by ASN or declared formally[76]. The time required to review the request for authorization is six months. ASN may extend this period if it judges that it is necessary to carry out further investigations or issue additional prescriptions. If ASN does not issue a response by the end of this period, the application is considered to be rejected;

– a 10-yearly review must be carried out by the operator, including for basic nuclear installations that are in the final shutdown or decommissioning phase.

e. Key documents associated with nuclear safety procedures

The expected content of some of the documents referred to below is, or will be, specified by ASN regulatory decisions (such as Decision 2015-DC-0532 on safety analysis reports for basic nuclear installations).

[75] This concerns modification, final shutdown and decommissioning of basic nuclear installations as well as subcontracting.

[76] Changes that do not significantly affect the safety analysis report or the impact assessment of the facility are covered by filing a (simple) declaration.

As indicated previously, the general conditions for issuing a construction authorization for a basic nuclear installation are based on 'protected interests' (security in the sense of French regulations, public health and hygiene, protection of nature and the environment). Thus, the information that the operator must submit to obtain a construction authorization is not limited to accident risk management, but also concerns limiting drawbacks inherent to operation (discharges, water intake, waste production, impact on flora and fauna, etc.). Moreover, the operator's ability to operate a facility is assessed not only on the basis of technical competence, but also on organizational, structural and financial aspects. The operator of a pressurized water reactor must envisage not only the operating phase of the facility, but also the future decommissioning phase and the financial provisions required.

The supporting information to be provided by the operator is described in a set of documents specified in Decree 2007-1557 of 2 November 2007 as amended[77], which identifies the purpose and content of each document. Most of these documents are analysed by IRSN at the request of ASN.

The various procedures to be applied from the initial design stage to decommissioning of a basic nuclear installation such as a pressurized water reactor are described in detail in Appendix 3.

▶ Safety Options Report

Prior to initiating the licensing process, any entity planning to operate a basic nuclear installation is offered the opportunity to request an opinion from ASN on all or some of the options it has selected to ensure the safety of the facility. EDF thus requested an opinion from ASN for the project known as the New Model European Pressurized Water Reactor (NM EPR)[78]. The submitted application, completed during IRSN's review, was examined at a meeting of the Advisory Committee for Reactors (Standing Group of Experts for Nuclear Reactors) in January 2018 and ASN issued its opinion in 2019.

▶ Safety Analysis Report

A safety analysis report, in a preliminary version, must accompany any construction authorization application for a basic nuclear installation. **The operator must demonstrate that the project achieves the lowest possible level of risk under economically**

[77] Amendments introduced by Decree 2016-846 of 28 June 2016 pertain to the following:
- framework for the use of subcontracting in the operation of basic nuclear installations,
- reform of the framework applicable to decommissioning basic nuclear installations,
- the implementation of more proportionate control of issues involved in significant changes to basic nuclear installations.

These amendments provide the regulatory stipulations required to incorporate the provisions of the TECV Act.

[78] Safety option reports have also been submitted to the safety authority for the Jules Horowitz Reactor and the ITER nuclear fusion project, two facilities under construction at Cadarache, as well as for the centralized storage pool that EDF plans to build by 2030 to accommodate spent fuel.

acceptable conditions, taking into account the current state of knowledge, practices and vulnerability of the environment at the facility location. This implies that the report must include an inventory of all risks of any origin that may exist within the planned facility; an analysis of the measures taken to prevent these risks; and a description of the means provided to reduce the probability of accidents and their consequences.

A 'design study' for the 'on-site emergency plan' (PUI)[79] must be submitted as part of the preliminary version of the safety analysis report. ASN Decision 2015-DC-0532 of 17 November 2015 (Safety Analysis Report Decision) indicates that this study:

- aims to identify, "among the accidents postulated in the safety demonstration"[80], those which, "despite preventive and mitigation measures, could lead to emergency situations and require protective measures on or off the site [...]" and "which must be brought to the attention of public authorities for the implementation of risk management policies within their jurisdiction [...];
- explains the principles for triggering the on-site emergency plan;
- identifies areas where the radiological emergency response levels specified in Article R.1333-80 of the Public Health Code or the thresholds for the effects of hazardous phenomena in Annex II of the Order of 29 September 2005 [...] could be exceeded;
- contains [...] the information needed to prepare the off-site emergency plan (PPI[81]) [...]; for this purpose, in scenarios requiring that public authorities take action immediately to protect the population, it specifies how the consequences will evolve within six hours after the beginning of the accident."

In practice, however, other information sources define the actual human and material resources associated with the on-site emergency plan, which are generally provided in the support documents that accompany this plan.

The safety analysis report is updated to obtain a fuel-loading permit[82] (i.e. for active commissioning, where nuclear or radioactive substances are used for the first time in the facility). The resulting updated safety analysis report serves to ensure that the facility complies with the construction authorization decree and any ASN prescriptions to be met in order to enact this decree, which authorizes facility design and construction. This implies that the safety analysis report must be based on the 'as-built' state of the facility.

The safety analysis report is also updated when the 'end-of-startup' report is submitted for final commissioning. It "describes any incidents and accidents reported

[79] *Plan d'urgence interne*.

[80] This does not include 'excluded' situations (see Chapters 6 and 17).

[81] *Plan particulier d'intervention*.

[82] ASN may authorize delivery of fuel within the boundary of the facility, without allowing fuel to be loaded into the reactor, by issuing a decision that authorizes what is referred to as 'partial commissioning'.

[…] since the operating authorization process began for the basic nuclear installation, as well as any curative, preventive and corrective actions taken, and summarizes any significant events that occurred, describing the manner in which each event was processed, from the beginning of startup until submission of the 'end-of-startup' report" This update must of course take into account the results of 'startup tests' (required for reactors in the French nuclear power plant fleet, which will be discussed in Chapter 19).

According to Subsection VII of Article 20 of the Procedures Decree, the safety analysis report shall be kept up to date, particularly in the following situations:

– if there is a change in the basic nuclear installation operator, or the operator's scope of responsibility, or if 'substantial' changes are made, i.e. changes that call into question compliance with the applicable decrees;

– when periodic reviews are conducted, which generally result in significant changes (see paragraph above), and when studies presented in the safety analysis report are updated.

▶ Risk Management Study

The risk management study presents the information contained in the preliminary version of the safety analysis report in a form appropriate for the local consultations and public inquiry called for in the construction authorization procedure.

▶ Impact Assessment

The impact assessment, which is part of the support documentation that accompanies any application for a construction authorization, describes how construction and normal operation of the facility will affect people and the environment. It is defined in Article 9 of Decree 2007-1557 mentioned above, and covers at least the following points:

– the radiological state of the site environment and its surroundings;

– an analysis of direct and indirect effects of the facility on the environment, which may be temporary (during the construction phase) or permanent;

– an assessment of the exposure of members of the public to ionizing radiation caused by the facility, taking into account irradiation caused directly by the facility and transfers of radionuclides through various pathways, including food chains. The planned water intake and discharge of liquid effluent into the environment or gaseous effluent into the atmosphere must be presented;

– the volume, type, detrimental effects and methods of disposal of radioactive and non-radioactive waste must also be described.

The impact assessment is also updated when the application for the operating authorization is submitted.

▶ Dismantling Plan

At the end of their operating lifetime, nuclear facilities are brought to the final shutdown state and must undergo preparatory and full dismantling operations before the site can be reused for another activity. The term 'dismantling' covers all activities carried out after final shutdown of a facility in order to reach a predefined end state. These operations typically include dismantling of equipment, cleanup of structures, possible destruction of civil works, cleanup of soil, and sorting, characterization, conditioning, removal and disposal of the waste produced (radioactive or otherwise). Following decommissioning, and under certain conditions, a basic nuclear installation is 'delicensed', meaning that it is removed from the list of basic nuclear installations.

Article L.593-25 of the French Environment Code stipulates that "When operation of a basic nuclear installation or part of such an installation is definitively stopped, the operator shall proceed with dismantling as soon as possible, under economically acceptable conditions and in compliance with the principles set out in Article L.1333-1 of the French Public Health Code and Section II of Article L.110-1 of the Environment Code." This strategy avoids placing the technical and financial burden of dismantling on future generations. It also makes it possible to take advantage of the knowledge and skills of the teams present during facility operation, which is essential during initial dismantling operations.

The dismantling plan, included in the support documents that accompany any construction authorization application for a basic nuclear installation, sets out the methodological principles and the stages envisaged for facility dismantling, remediation and subsequent monitoring of the site. In general, (see ASN Guide No. 6), the Dismantling Plan:

– "explains the methods envisaged for dismantling the facility and, if applicable, the methods for the remediation and monitoring of the site;

– details and substantiates the dismantling strategy chosen by the licensee [...] and describes the expected duration between the final shutdown of the facility and the end of its dismantling. This duration covers the time between final shutdown and the start of the dismantling operations as well as the duration of the operations themselves;

– defines and substantiates the state of the plant, both at the moment of final shutdown and when dismantling operations begin (initial state). It also defines and substantiates the expected end state of the site once dismantling of the plant has been completed [...];

– describes the measures taken by the licensee to preserve the history of the facility, including relevant information pertaining to its subsequent dismantling (i.e. radioactive and hazardous substances used, radiological maps, events, etc.) [...]."

After the construction authorization application has been submitted for a basic nuclear installation, the dismantling plan is updated in compliance with the Basic Nuclear Installation Order:

– when the facility is set into operation;

– whenever a change is made to the construction authorization;

– if necessary, when any change is made to the facility;

– each time a periodic review report is submitted (including during the decommissioning phase).

Specific safety issues related to dismantling operations will not be addressed in this book[83].

▶ Technical and Financial Capacity Statement

In order to obtain a construction authorization, the operator must provide a statement presenting its technical and financial resources. This statement, which is not made available to the public during the public inquiry, is intended in particular to substantiate the applicant's ability to exercise its responsibilities as a nuclear licensee on a long-term basis.

▶ General Operating Rules

The purpose of the General Operating Rules (RGE[84]) is to present the technical and organizational provisions adopted by the operator in line with the safety analysis report. Together with the safety analysis report, on-site emergency plan and waste management study, general operating rules are included in the documents to be submitted when applying for the facility operating authorization. They are updated as necessary to take into account changes, or evolving operating practices, as well as modifications in operations conducted from the beginning of decommissioning to the end of delicensing.

▶ On-site Emergency Plan

An on-site emergency plan (PUI) must also be submitted in order to authorize operation of a basic nuclear installation. This plan defines the organizational measures, intervention methods and means to be implemented by the operator[85] in emergency situations to protect personnel, the public and the environment from ionizing radiation and to maintain or restore facility safety.

ASN Decision 2017-DC-592 of 13 June 2017 sets out obligations regarding emergency preparedness and response and the content of the on-site emergency plan. This will be discussed in further detail in Section 17.9.

[83] For further information, see the CEA monograph *L'assainissement-démantèlement des installations nucléaires* (Cleanup and Dismantling of Nuclear Facilities), *Éditions du Moniteur*, 2018.

[84] *Règles générales d'exploitation*.

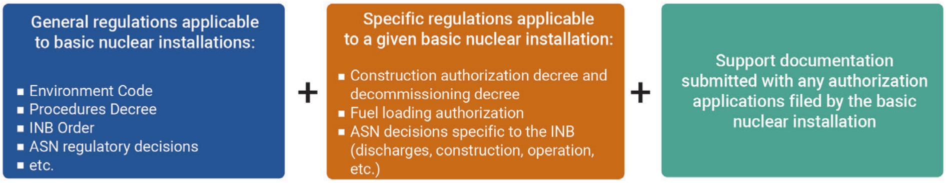
[85] The measures implemented outside the facility site where the accident occurred in order to protect the public and the environment are the responsibility of the prefect of the *département* concerned and are covered in the Off-site Emergency Plan, established to be coherent with the operator's On-site Emergency Plan (see Chapter 38 on emergency response management).

▶ Waste Management Study

A waste management study is part of the file to be submitted by the operator when applying for the facility operating authorization. It states the objectives set by the operator to limit the volume and radiological, chemical and biological toxicity of waste generated at the basic nuclear installation and to reduce the volume and activity of the final waste for disposal by applying appropriate recovery and treatment processes. This study describes all waste management solutions to be used at the facility, all the way to disposal.

f. Conclusion

The regulatory framework (or 'baseline'[86]) of a facility thus includes legally binding texts. Failure to comply with any regulatory provision constitutes a deviation that may result in an administrative or criminal penalty[87]. This can be illustrated as follows (Figure 2.4):



General regulations applicable to basic nuclear installations:

- Environment Code
- Procedures Decree
- INB Order
- ASN regulatory decisions
- etc.

+

Specific regulations applicable to a given basic nuclear installation:

- Construction authorization decree and decommissioning decree
- Fuel loading authorization
- ASN decisions specific to the INB (discharges, construction, operation, etc.)

+

Support documentation submitted with any authorization applications filed by the basic nuclear installation

Figure 2.4. Regulatory framework for a basic nuclear installation. Georges Goué/IRSN.

As discussed earlier, a decree must be passed to authorize construction or decommissioning of a basic nuclear installation; it also authorizes discharges (subject to compliance with the impact assessment). The decree mentions certain details such as the maximum capacity of the facility, the maximum duration of commissioning and the 'essential elements to safeguard protected interests' (public security, health and hygiene, protection of nature and the environment): **these elements are sufficiently important to constitute essential conditions for issuing an authorization; if any of these elements are jeopardized, a new application must be submitted for authorization**. The identification of these elements takes into account the specific characteristics of the facility, its risks and drawbacks.

[86] The term 'baseline' is widely used in the field of nuclear safety. It designates the codes and documents considered, particularly by operators and safety organizations, as safety requirements that must be met by the operator (the regulatory 'baseline') or requirements that the operator proposes and that become binding once they have been approved by safety organizations.

[87] For example, Areva was fined in October 2010 for failing to comply with the regulatory obligation to report an event without delay; the event involved a uranium leak that occurred on 8 July 2008 at the Socatri plant at Areva's Tricastin site. Similarly, for an event that occurred at the Plutonium Technology Plant (ATPu) at the Cadarache centre (underestimation of plutonium retention) in October 2009, CEA was fined in March 2012.

In addition to general regulations, ASN may also apply individual technical prescriptions to a basic nuclear installation, with regard to:

- incident and accident prevention,
- waste management,
- the need for the operator to obtain a specific authorization before conducting certain operations, in view of their importance,
- the procedures applied for water intake and consumption, liquid and gaseous effluent discharge into the environment and environmental monitoring.

Since compliance with regulations is not sufficient to demonstrate facility safety and, moreover, since regulatory requirements are formulated in terms of objectives to be achieved, assessing the management of risks and drawbacks is based on a continuous technical dialogue between the operator and safety organizations, with a case-by-case analysis of the organizational and technical measures that have been adopted.

#FOCUS

From the 1926 and 1943 decrees to the Nuclear Pressure Equipment Order: regulation of nuclear pressure equipment and state control of enforcement[88]

Pressurized water reactors, like other nuclear reactors, feature equipment (tanks or vessels, piping, etc.) containing reactor coolant (water, steam) at high pressure or temperature. This includes equipment such as the reactor vessel, the main primary system, main secondary system, pressurizer and steam generators. In the main primary system, for example, pressure reaches 155 bars and temperature about 300°C. These operating conditions obviously require special requirements to minimize the risk of loss of integrity by giving due consideration to possible alterations in the materials used.

Before construction of the first nuclear power reactors in France (gas-cooled reactors), equipment containing pressurized fluids was regulated by two texts: a decree of 2 April 1926 for 'steam pressure equipment'[89] and a decree of 18 January 1943 for 'gas pressure equipment'[90]. The 1926 decree applied

[88] The ASN news bulletin *Contrôle* Review No. 186, February 2010, (particularly the article by Sébastien Limousin) as well as Chapter 6 of P. Saint Raymond's book *Une longue marche vers l'indépendance et la transparence. L'histoire de l'Autorité de sûreté nucléaire française* (*La Documentation française*, 2012) served as the main sources for this Focus feature.

[89] Subsequently amended by decrees issued in 1928, 1929, 1961 and 1967.

[90] Subsequently amended by decrees issued in 1948, 1961, 1967 and 1977.

particularly to steam ‘generators’ (or ‘boilers’) and ‘vessels’, where pressure could exceed 0.5 bar and capacity could reach more than 25 litres (for generators) or 100 litres (for vessels). To ensure safe operation of this equipment[91], each item was subjected to a hydraulic test at a pressure that exceeded the normal operating pressure (generally 1.5 times the service pressure).

The application of these decrees to nuclear power reactors raised problems, first for GCRs, then for the first pressurized water reactor plant units under licence from Westinghouse: for PWRs[92], pressure vessels (especially those in the main primary system) needed to comply with US regulations, which, in turn, were based on the design and construction rules of the ASME code; whereas French decrees were based on another approach, which is still in force. This approach does not establish prescriptive technical instructions, but instead, stipulates that those responsible for designing and manufacturing pressure equipment must demonstrate that any potential risks that could apply to the equipment (such as the risk of sudden rupture), have been precluded. The decrees therefore do not prescribe compliance with any particular design and construction code[93].

The problem posed for pressurized water reactors[94] led to the Order of 26 February 1974 from the Minister for Industrial and Scientific Development, enacting application of pressure equipment regulations to nuclear steam supply systems – specifically to the main primary system (annexed by a circular dated the same day commenting on the provisions of the order). This order made certain adjustments to the 1926 decree in terms of test pressure. Precautions to be taken with regard to certain damage mechanisms were also introduced in the form of safety coefficients, which must be applied to the design loads calculated for the equipment item concerned. The 1974 order was prepared by a working group of industry specialists (in design, manufacture and inspection of pressure equipment, including Framatome, EDF and CEA) and the Technical Service of Mines (*Service technique des mines*), which in 1970 became the Directorate of Technology, Industrial Environment and Mines (*Direction de la technologie, de l’environnement industriel et des mines*, DITEIM).

In addition to the 1974 order, it was later considered necessary to extend the regulatory framework with fundamental safety rule II.3.8 of 8 June 1990 relative

[91] In addition to a few restrictions on the choice of materials and the need to equip ‘boilers’ with at least two safety valves.

[92] For GCRs, the two decrees of 1926 and 1943 appeared unsuitable for prestressed concrete containment structures, as they were written for metal tanks.

[93] These differences can be illustrated, for example, by the practice in the USA of affixing the ASME ‘N-stamp’ on equipment, which does not come under the responsibility of the U.S. NRC, whereas in France, a mark referred to as the ‘horse-head’ stamp was for a long time the sign that State inspection bodies recognized the equipment as being in compliance with regulations. As of 2019, the Nuclear Pressure Equipment Order no longer requires a horse-head stamp as in the past (see change in Section II of Article 6).

[94] The problem encountered for GCRs led to the publication of the decree of 15 June 1970 concerning prestressed concrete nuclear reactor structures.

to “the construction and operation of the main secondary system” of pressurized water reactors, which covers a certain number of aspects related to the design itself (choice of materials, rules and criteria of the RCC-M code to be applied with regard to the different loading situations, etc.). This fundamental safety rule was applied when reactor design for the N4 power plant series began.

In the 1990s, reactor operating experience feedback and international technical advances, particularly in non-destructive testing, led to a revision of requirements applicable to operation of reactor systems. Since it appeared that the main secondary system played a role just as important to nuclear safety as the main primary system, specific requirements, common to both the main primary system and the main secondary system, were then defined in an order issued on 10 November 1999, “on monitoring operation of the main primary system and main secondary system of pressurized water reactors” (referred to as the ‘Operation Order’).

In 1997, at the European level, Directive 97/23/EC, “on the approximation of the laws of Member States concerning pressure equipment” prescribed a new European approach to the regulation of ‘conventional’ pressure equipment, excluding from its scope equipment specially designed for nuclear applications. The three pillars of this European directive are the concept of ‘essential safety requirements’ for pressure equipment; the assessment of compliance with these requirements; and the existence of a body that conducts this assessment. This directive was initially transposed into French law by a new decree, Decree 99-1046 of 13 December 1999 (the Pressure Equipment Decree), relating to pressure equipment – with the exception of equipment designed for nuclear applications – which includes the concept of essential safety requirements introduced by the European directive.

The French government then decided, however, to use the 1997 European directive as a basis for reforming all its regulations on pressure equipment used in basic nuclear installations. This led to the Order of 12 December 2005 relative to nuclear pressure equipment, known as the Nuclear Pressure Equipment Order. The new order places this equipment in the same context as ‘conventional’ pressure equipment, but adapts it to the nuclear safety and radiation protection context, given the risks involved due to the radioactivity contained in the equipment.

The Nuclear Pressure Equipment Order contains not only the essential safety requirements for ‘conventional’ pressure equipment from the 1999 Pressure Equipment Decree, but also features additional provisions reinforcing risk analyses, qualification procedures, inspections and checks for nuclear pressure equipment. The Nuclear Pressure Equipment Order implements a unified approach commensurate with the relevant risks for all nuclear pressure equipment, taking into account, for each item of equipment:

- the pressure and volume of the fluid(s) contained in the equipment,
- the type of fluid(s) contained,

- the radiological inventory contained or likely to be contained in the equipment in operation,
- whether or not failure of the item has been taken into account in the safety demonstration of the facility in question.

The Nuclear Pressure Equipment Order thus defines a certain number of essential safety requirements for equipment, commensurate with the inherent risks, whereas equipment subject to less risk must simply comply with rules of the trade or professional guidelines.

The Nuclear Pressure Equipment Order makes certain additions or modifications to the Operation Order of 10 November 1999, and to the Decree of 13 December 1999 mentioned above. It replaces the Order of 26 February 1974 and the associated enactment circular.

The above-mentioned European directive was subsequently reformed by Directive 2014/68/EU of 15 May 2014 "on the harmonization of the laws of the Member States relating to the making available on the market of pressure equipment". The new directive has led to incorporation of the Pressure Equipment Decree in the French Environment Code and an update of the Nuclear Pressure Equipment Order by the Order of 30 December 2015 (pertaining mainly to design and manufacture), amended in a supplementary order (involving mainly in-service monitoring[95]) dated 3 September 2018. Essentially, these new orders are intended to leave current legislation unchanged, except for the 2015 order which, in application of the Environment Code, introduces a possible concession (Article 9) and a new transitional provision for application of the order (Article 12), and the 2018 order, which adds two new requirements resulting from recent feedback on component manufacturing[96].

Another text of interest is Decree 2015-799 concerning hazardous products and equipment, adopted on 1 July 2015 to transpose several European Union directives into national law, including the 2014 directive mentioned above, with a view to tightening regulations on hazardous products and equipment, such as explosive products, protective equipment and systems intended for use in a potentially explosive atmosphere, pressure equipment, and equipment and materials required for the use of combustible gases. This decree lays down the conditions for manufacturing and marketing these products and equipment, as well as rules for overseeing the market and in-service operations. In particular, it defines

[95] The 2018 order thus modifies the Nuclear Pressure Equipment Order and the Order of 10 November 1999.

[96] The Order of 3 September 2018 introduced new requirements related to feedback from recent cases. Two new requirements are noteworthy: conducting tests in accredited laboratories and the preservation of materials. The first results from tests performed inappropriately in the laboratories of certain manufacturers and recognition of the risk of fraud. The second comes in response to problems encountered with certain support documents that had to be based on 'representative' specimens rather than on material kept by the manufacturer from the part that was actually in service.

the responsibilities of the various economic operators, such as manufacturers, agents, distributors and importers. Decree 2015-799 of 1 July 2015 repeals the decrees of 1926 and 1943.

In the current situation, with the provisions for operation and in-service monitoring of pressure equipment and nuclear pressure equipment incorporated in the French Environment Code in 2016[97], the requirements applicable to design, manufacture, operation and in-service monitoring of pressure equipment are included in the following (see Figure 2.5):

- the French Environment Code, Chapter VII of Title V, Book V relating to 'hazardous products and equipment' in Section 9 (new pressure equipment), Section 12 (new nuclear pressure equipment) and Section 14 (operation and in-service monitoring of nuclear and non-nuclear pressure equipment);
- the Operation Order (1999) and the Nuclear Pressure Equipment Order (2015), amended in 2018, as well as the Order of 20 November 2017 'on in-service monitoring of pressure equipment and simple pressure vessels'.

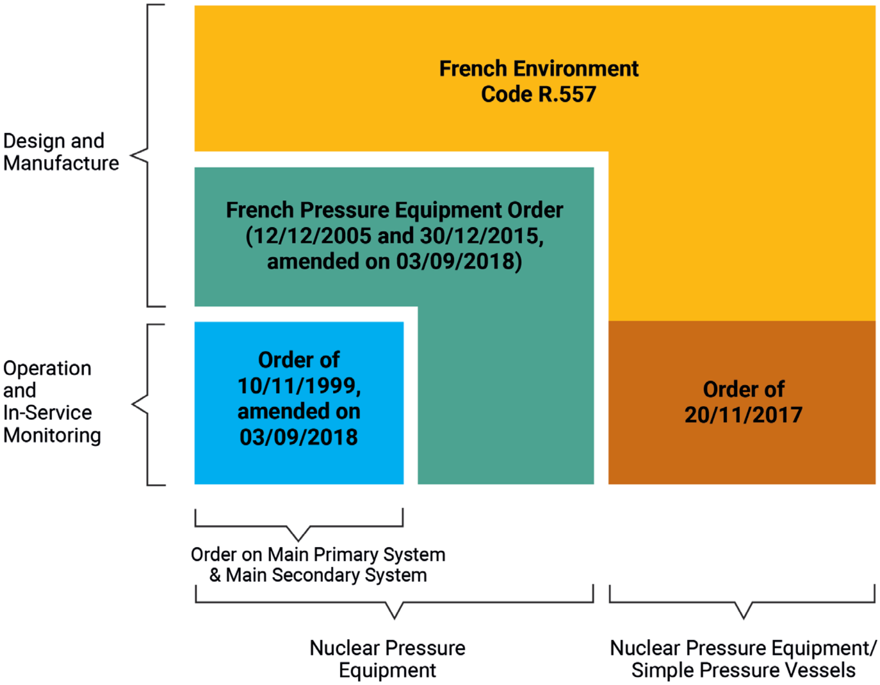

French Environment Code R.557
Design and Manufacture
French Pressure Equipment Order (12/12/2005 and 30/12/2015, amended on 03/09/2018)
Operation and In-Service Monitoring
Order of 10/11/1999, amended on 03/09/2018
Order of 20/11/2017
Order on Main Primary System & Main Secondary System
Nuclear Pressure Equipment
Nuclear Pressure Equipment/ Simple Pressure Vessels

Figure 2.5. Regulatory framework for pressure equipment, simple pressure vessels and nuclear pressure equipment. ASN/DEP.

[97] These provisions were incorporated in Decree 2016-1925 of 28 December 2016 relevant to in-service monitoring of pressure equipment.

ASN Decision 2016-DC-0571 of 11 October 2016, called for by the 2015 Nuclear Pressure Equipment Order, includes adjustments to certain points in the 2014 European directive and details concerning the Environment Code.

ASN has released two guides:

- ASN Guide No. 8 of 4 September 2012, which sets out the principles and procedures for the intervention of inspection agencies and bodies approved[98] by ASN for assessing compliance of nuclear pressure equipment and assemblies containing pressure equipment. It sets out the actions to be taken by manufacturers and operators of nuclear pressure equipment to ensure that the provisions concerning inspection agencies and bodies are applied correctly;
- ASN Guide No. 19 of 21 February 2013, which, after the first years of application of the Nuclear Pressure Equipment Order of 12 December 2005, sets out enactment procedures for achieving the objectives defined by the order, in response to needs expressed by manufacturers, operators and inspection bodies.

Furthermore, the French Association for Rules Governing the Design, Construction and In-service Monitoring of Equipment for Nuclear Steam Supply Systems (*Association française pour les règles de conception, de construction et de surveillance en exploitation des matériels des chaudières électronucléaires*, AFCEN) has issued several professional guides[99] for pressure equipment used in nuclear steam supply systems.

Further details about nuclear pressure equipment design are discussed in Section 8.6 and in-service monitoring is approached in the introduction to Chapter 26.

Application of the 1926 and 1943 decrees was historically the responsibility of the *Service des mines*, represented in France by district administrative offices that could either carry out the regulatory tests themselves or delegate them to independent experts such as the Association of Owners of Steam and Electrical Devices (*Association des propriétaires d'appareils à vapeur et électriques*, Apave). In 1974, the Director of DITEIM decided to entrust all inspections required by the 1974 order to the head of the Dijon district, since the most important components of nuclear reactors were built in the Burgundy region, and a dedicated agency was created for this purpose, the French Inspectorate of Nuclear Steam Supply Systems (*Bureau de contrôle des chaudières nucléaires*, BCCN). Later, with the creation of ASN in 2006, BCCN became the Nuclear Pressure Equipment Department (*Direction des équipements sous pression nucléaires*, DEP) within ASN.

[98] In Decree 2015-799 of 1 July 2015, the expression used is '*organismes habilités*' (state-approved conformity assessment bodies).

[99] They are part of the AFCEN Technical Publications series. AFCEN also distributes RCC codes, including RCC-M (Design and Manufacturing) and RSE-M (In-service Inspection Rules) for mechanical equipment.

The scope of control by the above bodies has expanded over time. Originally limited to the inspection of the design and construction of the main primary system on pressurized water reactors, it was extended in 1990 to include the main secondary system and then in 1994 to in-service monitoring of these two systems. The Nuclear Pressure Equipment Order extended the scope of inspection even further, covering not only the shell of nuclear pressure equipment, but also all the other parts.

DEP is responsible for:

- developing applicable regulations and the ASN doctrine adopted to enforce them;
- checking that regulations are applied (by manufacturers, designers, operators, etc.) in the construction of nuclear pressure equipment, principally by conducting inspections on the premises of equipment manufacturers (and their subcontractors) and verifying that equipment design and manufacturing documents comply with regulations;
- checking regulatory compliance of standard maintenance files for in-service equipment;
- supporting the efforts of ASN's regional divisions during unit outages, especially with regard to maintenance on main systems that are important to safety in nuclear power plants.

DEP establishes the conformity of the most important items of nuclear pressure equipment (belonging to level N1 according to the Nuclear Pressure Equipment Order). For other nuclear pressure equipment, this task comes under the responsibility of state-approved conformity assessment bodies. For this purpose, DEP reviews applications from organizations wishing to carry out regulatory inspections on nuclear pressure equipment and decides on their certification, particularly by conducting audits.

Appendix 1. Fundamental safety rules

Fundamental safety rules for Pressurized Water Reactors

I-2-a *Prise en compte des risques liés aux chutes d'avion* (Taking into Account Risks Associated with Aeroplane Crashes), 5 August 1980

I-2-b *Prise en compte des risques d'émission de projectiles par suite de l'éclatement des groupes turboalternateurs* (Taking into Account the Risk of Projectile Generation Following the Explosion of Turbine Generator Units), 5 August 1980

I-2-c *Détermination des mouvements sismiques à prendre en compte pour la sûreté des installations* (Determination of the Seismic Motion to be Taken into Account for the Safety of Major Nuclear Facilities), 1 October 1981, replaced by RFS-2001-01, in French

I-2-d *Prise en compte des risques liés à l'environnement industriel et aux voies de communication* (Taking into Account Risks Related to the Industrial Environment and Transport Corridors), 7 May 1982

I-2-e *Prise en compte du risque d'inondation d'origine externe* (Taking into Account the Risk of Flooding from External Sources), 12 April 1984, replaced by ASN Guide No. 13, Protection of Basic Nuclear Installations Against External Flooding, 8 January 2013

I-3-a *Utilisation du critère de défaillance unique dans les analyses de sûreté* (Using Single-Failure Criterion in Safety Analysis), 5 August 1980

I-3-b *Instrumentation sismique* (Seismic Instrumentation), 8 June 1984

I-3-c *Études géologiques et géotechniques du site ; détermination des caractéristiques des sols et études du comportement des terrains* (Geological and Geotechnical Site Studies; Determination of Soil Characteristics and Study of Soil Behaviour), 1 August 1985

II-2-2-a *Conception du système d'aspersion de l'enceinte*, (Containment Spray System), Revision 1, 31 December 1985

II.4.1.a *Logiciels des systèmes électriques classés de sûreté* (Software for Safety-Grade Electrical Systems), 15 May 2000

IV-1-a *Classement des matériels mécaniques, systèmes électriques, structures et ouvrages de génie civil* (Classification of Mechanical Equipment, Electrical Systems, Civil Works and Structures), 21 December 1984

IV-2-a *Exigences à prendre en compte dans la conception des matériels mécaniques classés de sûreté, véhiculant ou contenant un fluide sous pression et classés de niveau 2 et 3* (Requirements to Be Taken into Account in Designing Safety-Grade Mechanical Equipment that Conveys or Contains a Pressurized Fluid and Is Classified as Level 2 or Level 3), 21 December 1984

IV-2-b *Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté* (Requirements to Be Taken into Account in the Design, Qualification, Implementation and Operation of Electrical Equipment Belonging to Safety-Grade Electrical Systems), 31 July 1985

V-1-a *Détermination de l'activité relâchée hors du combustible à prendre en compte dans les études de sûreté relatives aux accidents* (Determination of the Activity Released from Fuel for Use in Safety Studies on Accident Situations), 18 January 1982

V-1-b *Moyens de mesures météorologiques* (Meteorological Instrumentation), 10 June 1982

V-2-b *Règles générales applicables à la réalisation des ouvrages de génie civil* (General Rules for the Construction of Civil Works – Conditions for Using RCC-G, January 1981 edition), 30 July 1981

V-2-c *Règles générales applicables à la réalisation des matériels mécaniques* (General Rules for the Construction of Mechanical Equipment – Conditions for Using RCC-M, July 1984 edition), Revision 1, 12 September 1986

V-2-d *Règles générales applicables à la réalisation des matériels électriques* (General Rules for Manufacturing Electrical Equipment – Conditions for Using RCC-E, Revision June 1984), Revision 1, 23 September 1986

V-2-e *Règles générales applicables à la réalisation des assemblages combustibles* (General Rules for Fabrication of Fuel Assemblies – Conditions for Using RCC-C, September 1989 edition), Revision 2, 14 December 1990

V-2-f *Règles générales relatives à la protection contre l'incendie* (General Rules for Fire Protection – Conditions for Using RCC-I, May 1982 Revision), 28 December 1982

V-2-g *Calculs sismiques des ouvrages de génie civil* (Seismic Design of Civil Works), 31 December 1985, superseded by ASN Guide No. ASN/2/01 (2006)

V-2-h *Règles générales applicables à la réalisation des ouvrages de génie civil* (General Rules for the Construction of Civil Works – Conditions for Using RCC-G, October 1985), 4 June 1986

V-2-j *Règles générales relatives à la protection contre l'incendie* (General Rules for Fire Protection – Conditions for Using RCC-I, October 1987 Revision), 21 November 1988

2001-01 *Détermination du risque sismique pour la sûreté des installations nucléaires de base de surface* (Calculating Seismic Risk for the Safety of Surface Basic Nuclear Installations), 31 May 2001

2002-1 *Développement et utilisation des études probabilistes de sûreté* (Development and Utilization of Probabilistic Safety Assessments), 26 December 2002

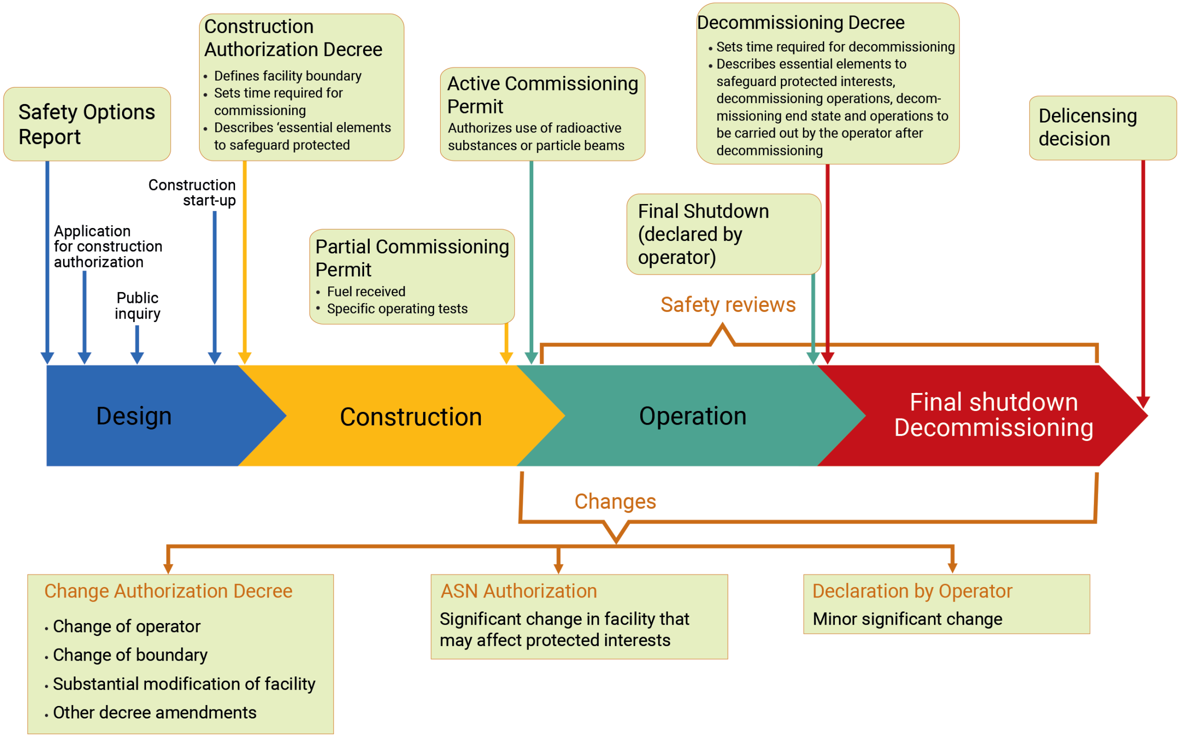
Appendix 2. Main Regulatory and Quasi-regulatory Texts Applicable to Pressurized Water Reactors (Excluding Pressure Equipment)

(as at December 2019)

- TSN Act of 13 June 2006 (enacted in the French Environment Code)
- Programme Act of 28 June 2006: On the Sustainable Management of Radioactive Materials and Waste (enacted in the French Environment Code)
- Decree 2007-830 of 11 May 2007: Nomenclature of Basic Nuclear Installations
- Decree 2007-1557 of 2 November 2007 as amended: Procedures for Basic Nuclear Installations
- Order of 7 February 2012 as amended: General Rules Applicable to Basic Nuclear Installations
- ASN Decision 2008-DC-0106 of 11 July 2008: Internal Authorization Systems
- ASN Decision 2012-DC-0236 of 3 May 2012: Spare Parts for Main Primary System and Main Secondary System
- ASN Decision 2013-DC-0360 of 16 July 2013: On the Control of Detrimental Effects and the Impact of Basic Nuclear Installations on Health and the Environment (as amended by Decision 2016-DC-0569 mentioned below)
- ASN Decision 2014-DC-0417 of 28 January 2014: Fire Risk Control
- ASN Decision 2014-DC-0420 of 13 February 2014: Changes to Basic Nuclear Installation Equipment
- ASN Decision 2014-DC-0444 of 15 July 2014: PWR Outage and Restart
- ASN Decision 2014-DC-0462 of 7 October 2014: Criticality
- ASN Decision 2015-DC-0508 of 21 April 2015: Waste Management Study and Report on Waste Generated in Basic Nuclear Installations
- ASN Decision 2015-DC-0523 of 29 September 2015: Classification of Basic Nuclear Installations with Regard to the Risks and Detrimental Effects They Represent for the Protected Interests Mentioned in Article L.593-1 of the French Environment Code

- ASN Decision 2015-DC-0532 of 17 November 2015: Safety Analysis Report
- ASN Decision 2016-DC-0569 of 29 September 2016: Management of Detrimental Effects and the Impact of Basic Nuclear Installations on Health and the Environment
- ASN Decision 2017-DC-588 of 6 April 2017: Procedures for Water Intake and Consumption, Effluent Discharge and Environmental Monitoring of Pressurized Water Reactors
- ASN Decision 2017-DC-592 of 13 June 2017: Obligations of Basic Nuclear Installation Operators Regarding Emergency Preparedness and Response and the Content of the On-site Emergency Plan
- ASN Decision 2017-DC-0616 of 30 November 2017: Significant Changes to Basic Nuclear Installations
- ASN Guide 2/01 of 26 May 2006: Considering Seismic Risk for Civil Works Design at Basic Nuclear Installations
- ASN Guide No. 3: Preparation of Annual Reports for Public Information
- ASN Guide No. 6: Final Shutdown, Decommissioning and Delicensing of Basic Nuclear Installations in France
- ASN Guide No. 9: Defining the Boundary of a Basic Nuclear Installation
- ASN Guide No. 11: Guide to the Declaration Procedure and Coding System for Criteria Concerning Significant Events
- ASN Guide No. 13: Protection of Basic Nuclear Installations Against External Flooding
- ASN Guide No. 14: Complete Post-operational Cleanup Methodologies Acceptable in Basic Nuclear Installations in France
- ASN Guide No. 15: Control of Activities in the Vicinity of Basic Nuclear Installations
- ASN Guide No. 21: Processing Non-compliance with a Requirement Defined for an Item Important to Protection on PWRs
- ASN Guide No. 22: Pressurized Water Reactor Design
- ASN Guide No. 23: Preparing and Amending the Waste Zoning Plan
- ASN Guide No. 24: Management of Soils Contaminated by the Activities of a Basic Nuclear Installation in France
- ASN Guide No. 34: Regulatory Requirements Applicable to On-site Transport Operations

Appendix 3. Procedures Applicable to Basic Nuclear Installations


Safety Options Report
Construction Authorization Decree
• Defines facility boundary
• Sets time required for commissioning
• Describes 'essential elements to safeguard protected
Active Commissioning Permit
Authorizes use of radioactive substances or particle beams
Decommissioning Decree
• Sets time required for decommissioning
• Describes essential elements to safeguard protected interests, decommissioning operations, decommissioning end state and operations to be carried out by the operator after decommissioning
Delicensing decision
Application for construction authorization
Public inquiry
Construction start-up
Partial Commissioning Permit
• Fuel received
• Specific operating tests
Final Shutdown (declared by operator)
Safety reviews
Design
Construction
Operation
Final shutdown Decommissioning
Changes
Change Authorization Decree
• Change of operator
• Change of boundary
• Substantial modification of facility
• Other decree amendments
ASN Authorization
Significant change in facility that may affect protected interests
Declaration by Operator
Minor significant change

Chapter 3
The International Dimension and the Social Dimension

3.1. International dimension

3.1.1. Introduction

This chapter does not aim to develop all the international aspects of nuclear safety and radiation protection, but simply presents a few noteworthy aspects, particularly concerning the safety of power reactors. For international aspects of security – in the sense of protection against malicious acts – and non-proliferation, the reader may refer to IRSN's book on these subjects[100].

Before exposing these highlights, however, a brief historical review appears necessary.

The first nuclear research and development programmes were carried out independently in several countries, sometimes combining research on nuclear power generation with developments focused on military applications. Confidentiality was thus the rule for strategic, political and commercial reasons.

The International Atomic Energy Agency (IAEA) was founded in 1957 by the United Nations with the main objective of promoting the peaceful use of nuclear energy and

[100] J. Jalouneix, Elements of Security and Non-Proliferation, Science and Technology Series, IRSN/EDP Sciences, 2017.

assisting Member States in this area by ensuring that IAEA support was not diverted towards military purposes. It was in the context of pressure from the USA to impose its regulations and practices, and thus its nuclear power industry, that lengthy discussions took place to define an organizational structure for the IAEA that would ensure the balance between nations in the ensuing developments. For those countries in the process of deciding to build nuclear power reactors, this did not in any way reduce the major contribution of the USA in the technical treatment of a certain number of nuclear safety issues, as will be seen several times in the rest of this book.

With regard to safety, in 1974, the IAEA began to develop a series of documents, known as 'standards', for the design and operation of thermal neutron reactors. For this purpose, it has gradually built a complete organizational structure in which representatives of designers, operators and safety organizations participate.

At the beginning of 2019, the IAEA had 171 Member States.

In 1958, the Nuclear Energy Agency (NEA) was also established within the Organisation for Economic Co-operation and Development (OECD)[101] to assist the Member Countries of the OECD in maintaining and further developing the scientific, technological and legal bases for a safe, peaceful and environmentally friendly use of nuclear energy. Within the NEA, a Committee on the Safety of Nuclear Installations (CSNI) was set up to deal with aspects relating to safety assessments and research.

As will be seen in Chapter 32, one of the consequences of the 1979 accident at Three Mile Island Unit 2 has been that incident analysis now takes a much broader view and has shown the value of asking how any given incident may become the precursor of a more severe accident. Following this accident, the NEA decided to set up a system for collecting, analysing and disseminating information among its members on particularly significant incidents affecting their nuclear facilities. The system has since been extended to the IAEA, which invites all nuclear countries in the world to participate.

In addition, more detailed discussions on safety matters have gradually developed between countries, either in the context of bilateral relations or in a broader framework.

For example, starting in 1972, France established relations with German safety organizations, since there were nuclear power plants in both countries located at a short distance from their common border.

Bilateral and multilateral relations have also multiplied to conduct studies and research in the field of safety. Those concerning pressurized water reactors in particular are covered in a separate IRSN publication[102].

[101] The OECD now includes all the countries of Western Europe, as well as the USA, Canada, Australia, South Korea and Japan.

[102] See J. Couturier and M. Schwarz, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2018.

Starting in the mid-1980s, the IAEA began to expand its nuclear safety activities by offering services closer to the facilities, particularly in developing countries, creating international teams 'on request'. At the invitation of a Member State, these teams directly examine how safety is effectively ensured during operation at the site selected by that State. These were first the Operational Safety Review Team (OSART) services, which deal with all the safety components in facility operation, followed by ASSET[103] services, which focus on incident analysis. Other services were developed subsequently and will be discussed later. These services do not constitute inspections; they provide an opportunity for discussions among peers that highlight satisfactory practices and recommendations for improvement. The reports are sent to the countries concerned, which decide whether or not to make them public.

The Chernobyl disaster in 1986 led to serious questions about the safety of nuclear facilities in former Soviet Union countries. In the 1990s, the political changes in these countries made it possible to visit their facilities, which led to a better understanding of their strengths and weaknesses, followed up by programmes to provide aid and transfer methods and technologies from Western countries.

Following the international conference on the Safety of Nuclear Energy – Strategy for the Future held in 1991 at the IAEA in Vienna, an international Convention was drawn up and adopted in June 1994. The Convention could only enter into force after ratification by a fixed number of Member States. Nearly 80 States signed the Convention. It has been effectively applied in France since it was ratified by the French Parliament on 26 June 1995. The Convention is devised to ensure that the individual IAEA Member States fulfil their safety responsibilities appropriately. Oversight is carried out by a Conference of the Parties (to the Convention) which meets regularly to review the reports provided by the various States under the Convention. The binding provision of the Convention is that each country must explicitly state how it implements the articles of the Convention.

Starting from the end of the 1990s, cooperation between countries grew quickly within a European framework (sometimes enlarged beyond European borders), between safety regulators (ENSREG[104], WENRA), and between Technical Safety Organizations (TSOs) with the EUROSAFE Forum and the ETSON network (these different entities will be described in greater detail later).

Of course, these international developments do not in any way reduce the responsibility of operators and national safety bodies.

Created after the Chernobyl accident, the activities carried out by WANO, which brings together the world's power reactor operators, will be briefly presented further on. Activities conducted by the INPO[105], however, as well as larger groups of electricity producers and distributors such as UNIPEDE[106] and EURELECTRIC, will not be

[103] Assessment of Safety-Significant Events Team.

[104] European Nuclear Safety Regulators Group (an advisory group of independent experts).

[105] Institute of Nuclear Power Operations.

[106] International Union of Producers and Distributors of Electrical Energy.

discussed here. These organizations are concerned, of course, with facility availability and production, but also, to a very large extent, with safety, and provide mutual assistance among operators.

3.1.2. IAEA standards

To promote the safe use of nuclear energy for peaceful purposes, the IAEA began in 1974 to draft a series of safety documents for its technical cooperation needs and to serve as a worldwide reference.

The legal status of the IAEA does not allow it to impose the application of these texts (except in return for its assistance). This would also be contrary to the prime responsibility of States, which is a fundamental principle in terms of safety.

The documents published by the IAEA follow a structure that has evolved over time. The current structure, shown below (see Figure 3.1), is pyramid-shaped.

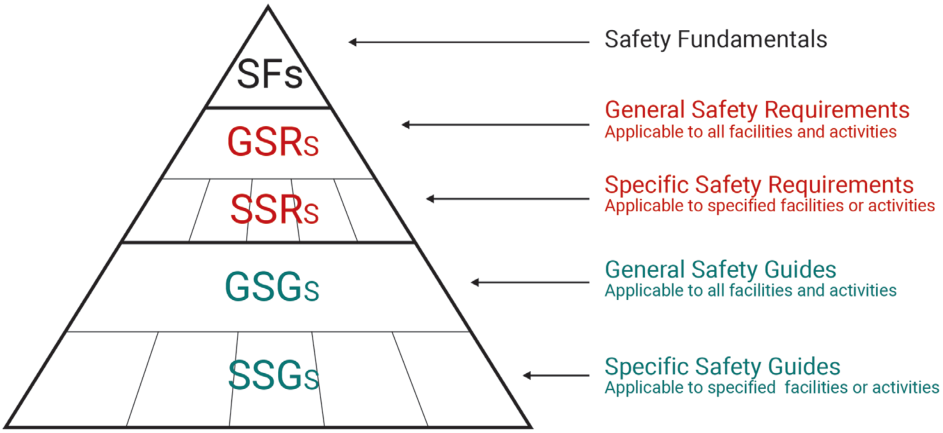

SFs
GSRs
SSRs
GSGs
SSGs
Safety Fundamentals
General Safety Requirements
Applicable to all facilities and activities
Specific Safety Requirements
Applicable to specified facilities or activities
General Safety Guides
Applicable to all facilities and activities
Specific Safety Guides
Applicable to specified facilities or activities

Figure 3.1. Architecture of IAEA safety standards (Safety Standards Series). IRSN (source: AIEA).

The top level[107] presents the Safety Fundamentals based on a general objective and principles of protection and safety that form the basis of Safety Requirements. Located at the second level of the pyramid, these requirements aim to protect people and the environment. The Safety Fundamentals and Safety Requirements are the result of an international consensus. At the bottom of the pyramid, safety guides provide recommendations and guidelines. Requirements and guides (see Figure 3.2) may be general in scope (General Safety Requirements/Guides), or specific to certain facilities (Specific Safety Requirements/Guides).

[107] Three documents in the Safety Fundamentals series were initially established by the IAEA between 1993 and 1995: the first on the safety of nuclear facilities, the second on waste management, and the third on radiation protection and the safety of radioactive sources. A new joint text was then drawn up in 2006, entitled Fundamental Safety Principles.

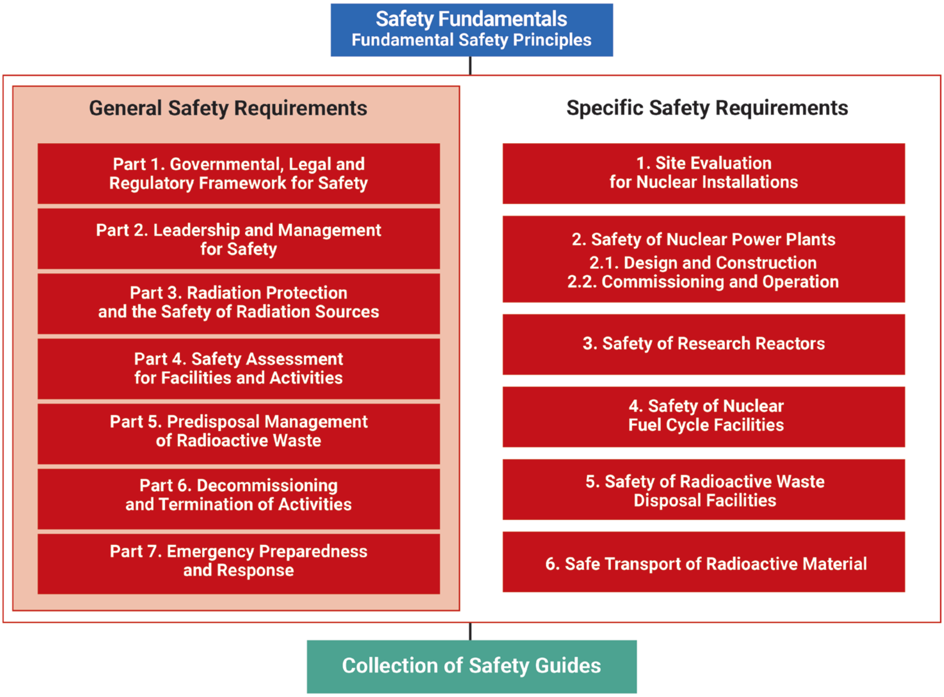

Safety Fundamentals
Fundamental Safety Principles
General Safety Requirements
Part 1. Governmental, Legal and Regulatory Framework for Safety
Part 2. Leadership and Management for Safety
Part 3. Radiation Protection and the Safety of Radiation Sources
Part 4. Safety Assessment for Facilities and Activities
Part 5. Predisposal Management of Radioactive Waste
Part 6. Decommissioning and Termination of Activities
Part 7. Emergency Preparedness and Response
Specific Safety Requirements
1. Site Evaluation for Nuclear Installations
2. Safety of Nuclear Power Plants
2.1. Design and Construction
2.2. Commissioning and Operation
3. Safety of Research Reactors
4. Safety of Nuclear Fuel Cycle Facilities
5. Safety of Radioactive Waste Disposal Facilities
6. Safe Transport of Radioactive Material
Collection of Safety Guides

Figure 3.2. Summary presentation of the fundamentals, requirements and guides issued by the IAEA. IAEA.

The differences in the design of facilities built by various manufacturers around the world did not simplify the preparation of these documents. It was indeed important that documents published under the auspices of an international organization should not, in fact, be mere descriptions of solutions adopted for a specific type of facility or a particular country. Any bias of this type would obviously have distorted competition on the relevant markets. The documents are intended to reflect an international consensus, not a catalogue of possible practices[108].

France, like other countries, was heavily involved in ensuring that the safety approaches it had adopted and developed were fully recognized.

Preparation and approval procedures have evolved over time, resulting in the current process: draft texts, prepared by small working groups, pass an internal quality control check and are reviewed by the IAEA Safety Standards Committees before being sent to Member States for formal consultation (only for Safety Fundamentals and

[108] Even though practices that are recognized as acceptable with regard to the set objectives may be mentioned or even described in certain documents, such as Guide SSG-25 on periodic safety reviews.

Safety Requirements) and are then approved by the IAEA Board of Governors[109]. There are four Committees that review the various IAEA draft texts and the comments made by Member States:

- the Nuclear Safety Standards Committee (NUSSC) for facility safety,
- the Radiation Safety Standards Committee (RASSC) for radiation protection,
- the Transport Safety Standards Committee (TRANSSC) for transport,
- the Waste Safety Standards Committee (WASSC) for waste.

These Committees are composed of high-level representatives of regulatory authorities, as well as other organizations that have observer status.

The draft texts are then submitted to the Commission on Safety Standards (CSS) before being approved by the Board of Governors.

The corpus of IAEA standards is gradually growing, and older texts are updated when necessary.

Another series of documents is also published by the IAEA, but within in a different framework. Following the Chernobyl accident, the IAEA Director General set up a high-level advisory group, the International Nuclear Safety Advisory Group (INSAG), which has about 15 members from various entities (industry – including both manufacturers and operators – regulatory authorities and technical organizations). It publishes recommendations that it prepares on subjects usually suggested by the IAEA, under its sole responsibility (INSAG experts do not represent their countries of origin).

As at late January 2019, INSAG has published 27 reports. The most widely known are INSAG-12, Basic Safety Principles for Nuclear Power Plants (a revision of INSAG-3), INSAG-10, Defence in Depth in Nuclear Safety, and INSAG-4 Safety Culture, supplemented by INSAG-13, which develops issues concerning organizations, and INSAG-15, which delves further into practical measures to improve safety culture.

INSAG, which initially dealt only with safety, has extended its scope to include radiation protection and other topics (INSAG 9: Potential Exposure in Nuclear Safety, INSAG 11: The Safe Management of Sources of Radiation: Principles and Strategies, INSAG 25: A Framework for an Integrated Risk-Informed Decision-Making Process, etc.).

INSAG-10 contributed largely to the presentation on defence in depth in Chapter 6 and INSAG-7 to analysis of the Chernobyl accident in Chapter 34 of this book.

3.1.3. International Reporting System for Operating Experience (IRS)

As mentioned above, in 1980, following the Three Mile Island accident, the NEA set up the Incident Reporting System (IRS) for the collection and dissemination of information on incidents occurring in the nuclear power reactors of its member coun-

[109] Which implies that the Member States agree to apply them (checks performed according to the Convention).

tries and likely to be of interest to these countries. The 33 countries belonging to the OECD/NEA (as of 2019) cover about 85% of the world's nuclear power capacity. In 1995, responsibility for management of the system was transferred to the IAEA and the system was opened to all countries that had signed the Convention on Nuclear Safety. Later, in 2009, to reflect the growing use of the system, the IRS became the International Reporting System for Operating Experience.

This process does not require that France submit to the IAEA and OECD/NEA information relating to all events declared to ASN, nor for France to receive and examine the equivalent information provided by other countries. That would submerge everyone in a mass of information of little importance from a safety point of view. Each country appoints a national coordinator for the IRS, who selects those incidents that they consider of sufficient interest to constitute lessons learned that can benefit other countries. In France, this mission is entrusted to IRSN.

At the end of January 2019, the IRS database contained 4332 reports; 421 of these were submitted by France, 1433 by the USA, 363 by Japan, 216 by Canada and 133 by Germany. The database also contained 171 documents issued by the former Soviet Union and 200 documents from the Russian Federation.

Regular meetings of national coordinators oversee the development of the system, the quality of the information submitted and technical improvements to the information systems used. They also focus on the lessons learned by each country from the challenges faced by other countries.

For example, a solution for treating the following problems was developed for French nuclear power plant reactors using information acquired through IRS:

– insufficient functional capacity of motorized valves,

– risk of clogging in sump filters,

– risk of corrosion and leakage on safety injection pipes,

– risk of cracking on the reactor coolant pump 'thermal barriers'[110].

The NEA, for its part, can set up working groups bringing together specialists from member countries to carry out studies on problems of general interest, based on a series of incident reports recorded in the joint IAEA-NEA IRS database, involving technical as well as human and organizational aspects. Several studies have been carried

[110] Leaktightness between the shaft of a reactor coolant pump and its motor is ensured by a system of several seals, into which water is injected at high pressure (from the chemical and volume control system, CVCS) in order to prevent water leakage from the reactor coolant system (RCS). Part of the water injected into the seals enters the RCS; the other part is collected and returned to specific systems (including CVCS). The seals are designed to function at temperatures that are lower than the coolant temperature in the RCS when the reactor is in operation. The thermal protection of these seals is ensured primarily by the water from the CVCS, which is injected at low temperature (by means of CVCS/CCWS [Component Cooling Water System] exchangers) and, in the event of failure of cold water injection, by a system referred to as the 'thermal barrier'. This system cools the coolant flowing through the thermal barrier to a temperature compatible with the maximum admissible temperature for the seals (90°C).

out in this manner, for example on incidents occurring during unit outages for refuelling and maintenance. More recently, following the Fukushima Daiichi nuclear power plant accident, the NEA conducted a review on a number of incidents and accidents considered to be precursors to possible core-melt accidents[111].

The IAEA also manages two other international databases relevant to incidents affecting research reactors (IRSRR – Incident Reporting System for Research Reactors) and fuel cycle installations (FINAS – Fuel Incident Notification and Analysis System).

The IRS, IRSRR and FINAS databases are accessible only to the Member States that supply them with data. All Member States do not necessarily submit their data in a uniform format.

A joint IAEA and NEA report from 2006[112] emphasizes that sharing operating experience requires constant efforts and vigilance: "Almost all of the events reported during that period [2002-2005] had already occurred earlier in one form or another. This shows that despite the existing exchange processes in place at both national and international levels, corrective measures, which are generally well-known, may not reach all end-users, or are not always applied strictly or in due time."

3.1.4. Services developed by the IAEA

Among the many services developed by the IAEA, two types of safety reviews conducted on the basis of IAEA standards are described below:

- reviews conducted by Operational Safety Review Teams (OSART), which consist of auditing the operational safety of nuclear facilities and activities,
- Integrated Regulatory Review Service (IRRS) reviews, which concern the regulatory systems for controlling nuclear activities (safety and radiation protection).

These safety reviews are carried out at the explicit request of the Member State concerned and are conducted by international teams formed specifically for the purpose of the corresponding mission.

3.1.4.1. OSART reviews

The principle of OSART reviews was adopted in 1982.

An OSART review team usually consists of 10 to 15 experienced people. Two thirds of them are external consultants, executives from nuclear power plants or safety organizations, some of whom may have already participated in this type of mission; the others are IAEA staff members. Some observers from developing nuclear countries

[111] From the Working Group on Operating Experience (WGOE): Report on Fukushima Daiichi NPP Precursor Events, NEA/CNRA/R(2014)1, January 2014.

[112] OECD Report 2006/NEA No. 6150 Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System, 2002-2005.

are associated with these missions. As a matter of principle, the experts on the team do not include anyone from the country being reviewed.

The external consultants selected, who vary from one mission to another, are chosen on the basis of their knowledge (type of reactor or technical speciality) and experience. The agency staff involved in these missions has similar professional experience. They ensure the consistency of mission objectives, criteria and results.

The team leader is an IAEA staff member. He or she is responsible for overall coordination, initial training of team members in the methodology used and overall orientation, as well as external media liaison.

An OSART review team typically spends three weeks at a facility.

The investigation programme is generally subdivided into several areas, explored in parallel:

- management, organization and administration of the facility,
- training, qualification and certification of personnel,
- control and operation of the facility,
- equipment maintenance,
- operating experience feedback, periodic testing, fuel management and handling,
- radiation protection,
- chemistry,
- emergency preparedness,
- managing core-melt accidents.

Technical exchanges between the members of an OSART review team and their counterparts at the nuclear power plant under inspection not only help to identify any problems, but also provide the opportunity to make comparisons with safety practices in other countries. This approach contributes to the dissemination of lessons learned and reflections on safety. Good practices may also be highlighted.

The report written by the review team at the conclusion of an OSART mission is sent to the country concerned, where the operator and regulatory authority are organized to make appropriate use of lessons learned. The report is usually made public by the regulator.

A follow-up inspection may be organized one or two years later to assess how the mission recommendations have been taken into account.

OSART reviews began in 1983. By the end of 2018, 204 missions had been carried out (covering 36 countries and 116 nuclear power plants), in addition to the 141 follow-up inspections.

In 1985, France hosted the first OSART review mission carried out in a developed nuclear country (on Unit 1 at the Tricastin power plant). Six French experts were part of the team (as required by France for this prototype experiment). Another OSART review was held in 1988 at the Saint-Alban–Saint-Maurice nuclear power plant.

EDF quickly realized the very positive impact of these reviews, due not only to the results of the reviews themselves and the benefit of an outsider's view of French practices, but also to the considerable involvement of all members of personnel throughout the preparation phase, a period particularly conducive to a more in-depth investigation of safety issues by the operator.

From its foundation, the French safety authority (DSIN) was in favour of this practice, demonstrating its willingness to open up the national nuclear safety control system to greater transparency.

France then decided to host an OSART review mission once every year in one of the country's nuclear power plants. Thus, from 1985 through 2017, 30 OSART reviews (and 24 follow-up inspections) were carried out in the nuclear power plant fleet (by the end of 2014, 26 OSART reviews had been conducted in France, 8 in the USA and 5 in Japan). The main findings of OSART reviews are generally available on the IAEA website[113].

The overall conclusions of the missions carried out in French nuclear power plants have always been favourable, but most often accompanied by a few questions, remarks or suggestions.

In the early years (1980s), the review teams frequently asked questions about the relatively centralized structure of EDF and the sharing of responsibilities and resources between the nuclear power plant sites and centralized corporate services. This question is partly explained by the fact that there is no other operator in the world with such a large-scale nuclear power plant fleet. The experts in the OSART review teams were therefore often surprised by the way EDF functioned when they inspected just one reactor.

Suggestions for improvement included, for example:

- better communication between management and personnel from operations and maintenance, as well as the presence of field supervisors,
- continuing education programmes and training evaluation procedures,
- ensuring plant sites are involved in corporate analysis of operating experience feedback,
- root-cause analysis of significant events (this continued to be recommended in the conclusions of OSART reviews conducted after 2011),

[113] They are also available on the ASN website for French nuclear power plants.

- follow-up on maintenance activities and their results,
- follow-up on temporary changes.

French engineers, usually from EDF and IRSN, have also participated as experts in OSART reviews in other countries, which, again, enlarges dissemination of lessons learned and stimulates reflection on safety issues.

Pre-Operational Safety Review Team (Pre-OSART) reviews may also be conducted during the construction and licensing phases of a nuclear facility.

3.1.4.2. IRRS reviews

A review by IRRS (corresponding to what was formerly known as the International Regulatory Review Team, IRRT) can be conducted at the request of a Member State who wishes to compare its own nuclear safety control system with IAEA standards. These reviews aim to improve the performance of safety control systems by encouraging authorities to share their experience with each other, while promoting good practices.

At France's request, a team of international auditors consisting of 24 experts coordinated by the IAEA visited ASN in 2006 to conduct the first comprehensive IRRS review in France. The purpose of the mission was:

- on one hand, to examine, according to the peer review principle, the national nuclear safety and radiation protection control systems with regard to the standards issued by the IAEA;
- on the other hand, to share knowledge and compare experiences between the auditors and all stakeholders in France involved in the governance of nuclear and radiological risks.

The auditors mainly examined regulatory, inspection and public information practices. They met with ASN teams, including those from its regional divisions, and IRSN teams, and assessed ASN's inspections by examining about ten that had been conducted in the field.

In 2014, a second IRRS mission took place in France[114] with the same objectives, according to new procedures implemented by the IAEA (self-assessment based on a questionnaire developed by the IAEA) and on a broader technical scope than the 2006 audit (which covered medical exposure, worker radiation protection, environmental protection and connections between safety and security).

Each of these IRRS reviews was accompanied by a follow-up mission, in 2006 and 2017, respectively[115].

[114] After the reorganization that led to the creation of ASN.

[115] IRRS mission reports are available on the ASN website.

3.1.4.3. Other services and study frameworks set up by the IAEA

The IAEA has established other services and frameworks for studies in addition to those described above.

Among these, a service associated with OSART reviews, called ISCA (Independent Safety Culture Assessment[116]), specializes in safety culture and its assessment. The INSAG-4 safety culture report served as the basis for a detailed guide (IAEA-TECDOC[117]-743), published in 1994, that set out to assess safety culture awareness and corresponding attitudes in the various organizations concerned. Given that this is a sensitive subject, the service initially focused on having the IAEA set up a training programme on how to use the safety culture guide and carry out the self-assessment.

Development of another service, SALTO (Safety Aspects of Long-Term Operation), began in 2005. The purpose of this service is to assist Member States in dealing with issues raised by 'long-term' operation of a nuclear facility, for example, in the case of extending the operating lifetime of a reactor. A certain number of aspects are addressed in the corresponding missions:

- managerial aspects,
- the safety 'baseline' (safety reference documents),
- ageing management of structures, systems and components (civil works, metal structures, mechanical components, instrumentation and control equipment, etc.),
- knowledge and human resource management.

In the context of extending the operating lifetime of Unit 1 up until 2025 at the Tihange nuclear power plant in Belgium (reactor commissioned in 1975), a SALTO mission was carried out in December 2015. A similar mission was also carried out for Doel Units 1 and 2 in February 2017[118].

Lastly, the IAEA has in the past[119] offered a service called the Assessment of Safety-Significant-Events Team (ASSET) to provide assistance in the in-depth analysis of safety-significant incidents occurring in nuclear power plants. Particular emphasis was placed on investigating the root causes of incidents, whether they were due to equipment, procedures, personnel or organization. These investigations showed that periodic tests were not conducted systematically or were not representative; that operating and maintenance documents were not approved and updated; and that the training of operating and maintenance personnel and even management was insufficient. Emphasis was also placed on corrective measures, which were not always taken adequately or promptly, and lessons learned were not distributed appropriately.

[116] This independent safety culture assessment service replaced the Assessment of Safety Culture in Organizations Team (ASCOT).

[117] TECDOCs are technical documents approved only by their authors.

[118] Mission reports are available at https://afcn.fgov.be.

[119] This service is no longer available.

The first ASSET mission took place in 1986, with several missions carried out in Eastern European countries.

In France, a team of this type was received at Gravelines 1 in 1990 following a maintenance anomaly that occurred in 1989 in this reactor[120]; another was received in 1992 at the Fessenheim nuclear power plant to examine the impact of feedback after ten years of operation; a third team visited the Paluel nuclear power plant in 1993 after an incident that led to diagnostic problems followed by reporting issues[121].

The ASSET teams had fewer experts than the OSART review teams and the inspection lasted only two weeks; the team members were selected in a way similar to that of the OSART review teams.

The overall conclusions of the ASSET missions conducted in France were generally favourable, with some remarks and suggestions that were usually similar to those made during the OSART reviews. Certain noteworthy suggestions included the following:

- a policy should be defined to maintain long-term efforts to promote a questioning attitude on the part of teams and individuals;
- site management should be more involved in setting priorities for equipment and organizational changes;
- training programmes should be revised to develop knowledge among relevant personnel members with regard to facility design and its effect on control operations;
- greater assistance should be provided to less experienced personnel, with better monitoring of each person's skills;
- more attention should be given to addressing the root causes of incidents;
- greater resources should be available on sites to solve certain recurring problems more quickly.

In 2000, a new service, called PROSPER (Peer Review of Operational Safety Performance Experience Review) was established, broadening the scope of ASSET reviews. This type of review is now conducted within the context of OSART missions.

The IAEA has also established various frameworks for studies and research, including Coordinated Research Projects (CRPs) and International Collaborative Standard Problems (ICSPs). This work has led to the preparation of technical documents called Safety Reports, Technical Documents (TECDOCs). TECDOCs have been published on subjects such as the assessment of 'passive systems'[122], approaches for managing equipment ageing, comparison of assessments by calculating the seismic behaviour of power reactors, evaluating 'advanced' thermal-hydraulic simulation software, etc.

[120] See Section 22.2.

[121] See Section 23.1.3.

[122] See Chapters 7 and 18.

3.1.5. WANO[123]

Created in 1989 following the accident at the Chernobyl nuclear power plant, the World Association of Nuclear Operators (WANO) is the international industry association exclusively dedicated to nuclear safety. WANO brings together the world's power reactor operators, and is also open to operators of spent fuel reprocessing plants.

Its purpose is to improve safety through exchanges and mutual support between operators via peer reviews, sharing operating experience feedback, dissemination of good practices, training and support missions.

Peer reviews form the backbone of WANO's action: each plant must undergo a peer review once every four years. For each review, about 25 operations specialists spend nearly three weeks on site to assess the quality and discipline exercised in operations, facility management, safety culture and operational management in the fundamental areas of safety. The review teams are international.

Based on field observations, fact gathering and interviews, the review identifies deviations from standards and best practices as well as the strengths and weaknesses of the site and indicates areas for improvement. An overall assessment of the site is finally pronounced and reported to corporate management. Following a review, the operator draws up an action plan and sends it to WANO; its concrete effects are checked two years later by a follow-up review. The action plan is supported by WANO's technical assistance missions. Nuclear power plants with safety deficiencies receive specific support and are monitored individually, with progress reported regularly to the WANO Board of Governors.

Each operator sends reports to WANO on incidents that may be of interest to the community. They are available to all members through a secure database and intranet site. The most important incidents, or topics derived from them, are written up in specific reports and recommendations issued by the association. Implementation of these recommendations is assessed in peer reviews.

WANO's staff consists of about 450 permanent employees, most of whom are seconded by operators for a few years. Peer reviews, technical missions and seminars are carried out by seconded employees with support from non-seconded members of the association, who intervene for the occasion. In addition to its headquarters in London, WANO is set up to cover four operational regions: Atlanta, Paris, Moscow and Tokyo.

WANO was significantly reinforced after the Fukushima Daiichi nuclear power plant accident: its workforce has tripled, peer reviews are conducted more frequently and cover a broader scope (preparedness for severe accidents, emergency response, certain elements involving facility design), operating crews are observed in simulated accident situations, corporate peer reviews are implemented, general coordination and

[123] Contribution by Bertrand de Buchère de l'Épinois, EDF, member of the Advisory Committee for Reactors.

consistency between regions has increased, and a new centre was opened in Shanghai, becoming WANO's second branch office in Asia.

WANO is a rather unique international organization in terms of the transparency achieved between potential competitors in electrical power generation and the ability to hold discussions without complacency. This openness has developed because confidentiality is guaranteed and members are convinced that collective responsibility for stimulating each other and advancing together has become an integral part of the individual responsibility of each operator. Through its presence in the field, its moral influence and the commitment of utility companies at corporate level, WANO has become a kind of 'internal regulator' or 'professional organization' for nuclear operators.

3.1.6. NEA

As mentioned previously, the mission of the NEA is to assist OECD member countries that join the NEA in maintaining and further developing the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes. It provides reference documents and brings differing views to a consensus on important issues, which can be used by governments in defining their nuclear policies, and contributes to more general studies conducted by the OECD on issues such as energy and sustainable development.

The NEA's scope of action includes nuclear safety, radioactive waste management, radiation protection, nuclear science, economic and technological aspects of the fuel cycle, nuclear law and liability, and public information.

The NEA has set up technical standing committees, mainly composed of experts and technicians from member countries. These committees constitute the unique character and driving force of the NEA, as they provide the flexibility required to address new issues and reach a consensus. There are seven technical standing committees:

– Committee on the Safety of Nuclear Installations (CSNI): its mission is to help member countries maintain and develop the scientific and technical knowledge needed to assess the safety of nuclear reactors and fuel cycle facilities. Its members consist of scientists and engineers with major responsibilities in various areas of technology and safety research (including experts from IRSN), as well as representatives of safety authorities;

– Committee on Nuclear Regulatory Activities (CNRA): it consists of representatives of nuclear safety authorities. Its mission is to lead the NEA's programme concerning regulations, licensing processes, inspection of nuclear facilities with regard to safety, and operating experience feedback (NEA's involvement in incident analysis, an activity assigned to the Working Group on Operating Experience (WGOE), was mentioned above);

– Radioactive Waste Management Committee (RWMC): its mission is to contribute to international cooperation in the management of radioactive materials and waste from facilities, including facility decommissioning and waste management over the long term;

- Committee on Radiological Protection and Public Health (CRPPH): the CRPPH is composed of representatives of radiation protection authorities and radiation protection experts. Its mission is to identify emerging issues in the field, analyse their possible implications and recommend or undertake action to address these issues and advance the regulation and implementation of radiation protection;
- Nuclear Science Committee (NSC): its mission is to assist member countries in identifying, collecting, developing and disseminating the scientific and technical knowledge necessary to ensure the safe, reliable and economical operation of existing nuclear facilities and to develop new-generation nuclear systems;
- Committee for Technical and Economic Studies on Nuclear Energy Development and the Fuel Cycle (or Nuclear Development Committee, NDC): its mission is to provide the governments of member countries with reliable information on nuclear energy technologies, economics, strategies (such as different fuel cycle strategies[124]) and resources, thus contributing to policy analysis and decisions, as well as the future role of nuclear energy in a sustainable development perspective and in the national and international context of energy policies;
- Nuclear Law Committee (NLC): its mission is to assist in the development of the national and international legal regimes required for the peaceful use of nuclear energy – including international trade in nuclear materials and equipment –, to address issues of liability and compensation for nuclear damage, and to serve as a centre for nuclear law information and education.

Nuclear safety is the main focus of CSNI's activities and part of those of NSC, which cover the following technical areas: neutron physics, criticality, thermal hydraulics, in-reactor fuel behaviour, accident physics (including core melting), behaviour of uranium–235 fission products contained in fuel, external 'hazards'[125], human and organizational factors and risk analyses. These activities involve exchanging technical knowledge, producing state-of-the-art reports, comparing analysis methods or different types of simulation software (based on benchmarks), and achieving consensus or shared views on identified research and development needs.

The NEA also manages a database that constitutes an international reference centre for member countries, providing basic tools used in the field of nuclear energy, such as simulation software and nuclear data. The centre provides direct services to its

[124] The fuel cycle refers to all operations involved in supplying fuel to nuclear reactors and then managing spent fuel, i.e. from ore extraction to radioactive waste management.

[125] As will be seen and developed in the rest of this book, the term 'hazards' covers events occurring inside or outside a facility that are not foreseen malfunctions of process-related systems in the facility, but rather situations corresponding either to external natural events (such as earthquake or flooding), events related to human activity (external explosion, etc.), or internal events such as fire, a dropped load, flooding caused by a pipe break, and others.

users by developing, enhancing and approving these tools and making them available on request.

Lastly, the NEA provides member countries with a framework for funding and implementing major international research programmes. As mentioned previously, the NEA was founded in 1958 to facilitate the implementation of such programmes and its early achievements were quite large-scale projects: Halden (beginning in 1958[126]), Dragon (1959-1976) and Eurochemic (1959-1975). Since 1980, the NEA has organized more than 50 joint projects (nearly 20 are on-going[127]) in the field of nuclear safety, including two-phase thermal hydraulics, fuel behaviour in accident situations, core-melt accidents and fires.

3.1.7. Organizations dedicated to radiation protection and health

So far we have seen that radiation protection and the impact of ionizing radiation on human health are part of the concerns and scope of activity of both the IAEA and NEA. But two other leading international organizations must also be mentioned: ICRP, the International Commission on Radiological Protection, and UNSCEAR, the United Nations Scientific Committee on the Effects of Atomic Radiation.

Introduced in Chapter 1, the ICRP, founded in 1928[128], before the IAEA and NEA existed, has played a leading role in establishing the major principles of radiation protection. Since the 2000s, the ICRP has extended the scope of its recommendations to environmental radiation protection, thereby including plants and animals. Experts from France, including IRSN staff, participate in the Main Commission, the governing body, as well as each of the four ICRP committees dealing respectively with radiation effects, doses from radiation exposure, radiological protection in medicine, application of recommendations on radiation protection principles and environmental protection. The director of the French Centre for the Study of Assessment of Nuclear Protection (*Centre d'étude sur l'évaluation de la protection dans le domaine nucléaire*, CEPN)[129] is a member of the Main Commission.

The United Nations General Assembly established UNSCEAR in 1955. The committee is mandated to collect, analyse and synthesize data from around the world on exposure levels and the effects of ionizing radiation. Its summary reports provide a scientific basis for assessing the risks associated with ionizing radiation and defining

[126] The final shutdown of the Halden reactor was decided in June 2018. Post-irradiation examinations and experiments on irradiated materials performed in 'hot' cells will nonetheless continue.

[127] Late January 2019.

[128] The ICRP, officially established in 1950 under this name, came from the International Committee for X ray and Radium Protection, established in 1928.

[129] This is an organization created in France 1976, whose partners are CEA, EDF and IRSN. This non-profit organization is a research and study centre in the nuclear field that assesses measures taken to protect people from the risks of ionizing radiation, taking into consideration technical, health, economic and social aspects.

protective measures. An important contribution of UNSCEAR involved work on the consequences of the 1986 Chernobyl power plant accident. Reference will be made to a number of its publications in Chapter 34, devoted to this accident. Along the same lines, UNSCEAR published a report in 2013 on the 2011 Fukushima Daiichi nuclear power plant accident[130].

The important activities of these two organizations will not be described further, given that the focus of this book is nuclear safety.

3.1.8. From bilateral Franco-German cooperation to European structures for the exchange and capitalization of knowledge and practices, training and assessment services

Since the 1970s, Franco-German cooperation has instigated the gradual development of European structures for sharing experience, conducting joint projects and harmonizing practices in safety assessment.

Relations between the German and French safety organizations began in 1972, shortly after the decision to build the Fessenheim nuclear power plant on the French side of the Rhine. They then intensified over time[131].

In 1976, a joint working group conducted a comparison between Fessenheim 1 and Neckarwestheim 1 and published their conclusions in 1977, before Neckarwestheim 1 was commissioned and shortly after commissioning of Fessenheim 1. These conclusions clearly express the novelty and, at the time, the difficulty of this type of exercise: "The study has shown that it is difficult to make a detailed, point-by-point, safety comparison in all areas when the systems themselves or their design bases are different. In both countries, the objectives set to ensure a high level of safety in nuclear power plants are generally similar. The safety of a nuclear power plant is ensured by a multitude of technical and organizational measures, not to mention quality assurance and control in the construction phase. In conclusion, it can be said that the technical safety requirements for the two facilities are comparable, but that the methods established to address safety issues are sometimes different. The means used to achieve similar objectives may legitimately vary, but are equally valid."

A report with similar conclusions, relating to the higher-power Cattenom and Philippsburg units, was issued in 1982.

[130] UNSCEAR 2013 Report – Scientific Annex A: Levels and Effects of Radiation Exposure due to the Nuclear Accident after the 2011 Great East-Japan Earthquake and Tsunami.

[131] From 1993 onwards, a representative of the German safety organizations was invited on a permanent basis to meetings of the French Advisory Committee for Reactor Safety (GPR) and, as of 1994, a French expert was appointed to its German counterpart, RSK (*Reactor-Sicherheitskommission*, the Reactor Safety Commission).

Such comparisons have examined, for example, how to ensure the best reliability of safety functions by using high levels of redundancy or functional diversification; or the detailed assumptions used in France and Germany to calculate the radiological consequences of accidents studied in safety analysis reports.

Franco-German cooperation continued with the creation of the Deutsche-Französische Kommission (DFK)[132] for questions involving the safety of nuclear facilities and, in 1990, the Deutsche-Französischer Direktionausschuss (DFD)[133], providing a national institutional framework for these collaborative efforts.

Then the Western nuclear countries gradually mobilized to improve safety in power plants located in Eastern European countries (see Figure 3.3), working both individually and through international action and financing.

The first joint assessments were carried out on reactor projects in East Germany (for the Greifswald power plant, already equipped with four 440 MWe VVER reactors from the 230 series, with four more reactors planned from the more recent 213 series, and the Stendal power plant, which was to have four 1000 MWe VVER reactors), projects which reunited Germany ultimately decided to abandon.

Next, following an IAEA mission in Bulgaria that had revealed the unsatisfactory state of operation of the Kozlodouy power plant, consisting of four first-generation 440 MWe VVER-type reactors (230 series), the decision was taken to help this country address the safety issues raised by the plant, as the Bulgarian government considered that continuing to operate these reactors was essential for the economic and social survival of the country, with the Russian designer supporting the idea that they were fit for operation.

IPSN was heavily involved in this support mission, together with GRS[134], working through the European economic interest group, RISKAUDIT IRSN/GRS International[135], a non-profit organization set up in 1992, while EDF helped the operator via WANO, in addition to a twinning arrangement set up between the nuclear power plants at Kozloduy (Bulgaria) and Bugey (France). While it was recognized that the 440 MWe VVER reactors featured some favourable safety aspects (such as high thermal inertia due to large amounts of reactor and secondary coolant,

[132] A Franco-Luxembourg commission and a Franco-Swiss commission have also been set up.

[133] Since the DFK (Franco-German Commission) was a regional structure (at least on the German side), it seemed necessary to create an organization to deal with general safety problems at the national level, which became the role of the DFD (Franco-German Management Committee) in 1990. DFD was a small group (excluding Länder representatives on the German side) for political reasons, as both governments were seeking to achieve close cooperation from an industrial viewpoint, between Framatome and Siemens, and from the assessment viewpoint, by bringing together experts from IPSN and GRS. The topics to be covered included, for example, nuclear safety in Eastern European countries and the European Pressurized water Reactor.

[134] Supported by European funding.

[135] Hereafter referred to as RISKAUDIT.

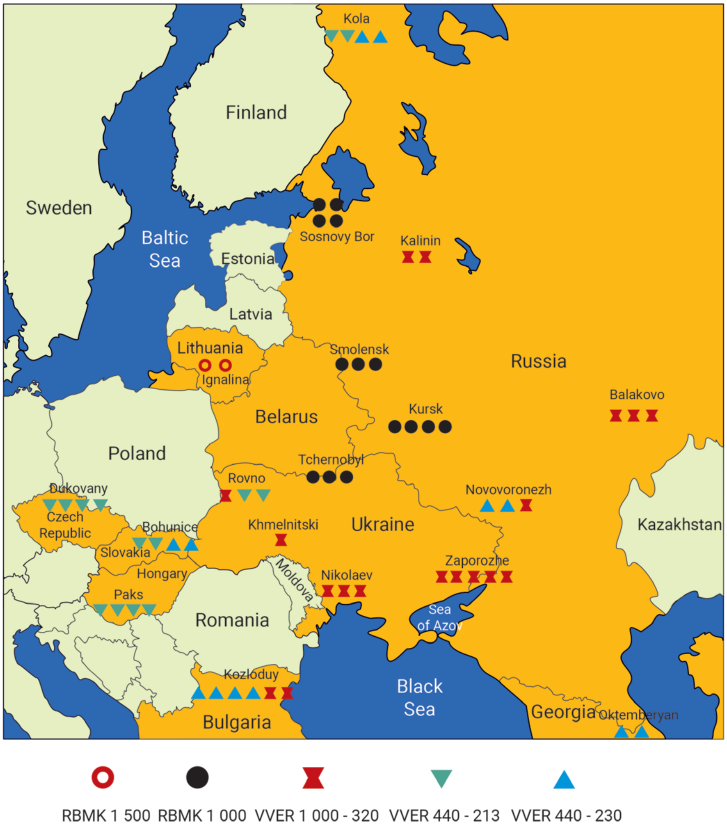


Figure 3.3. Nuclear power plants in the former USSR and Eastern Europe in the mid-1990s. Georges Goué/IRSN.

low linear power density fuel, and the ability to manually isolate the reactor coolant loops in the event of steam generator tube rupture, etc.), the experts identified several areas of concern, including:

- a risk of sudden vessel rupture due to irradiation embrittlement of the weld metal, particularly for certain VVER 440/230 reactors. This was due to significantly higher levels of impurities (especially copper and phosphorus) in this material than in western pressurized water reactors. Annealing, which had already been performed, was again necessary to 'erase' the defects created by irradiation of the weld metal;
- design of the VVER 440/230 plant units, characterized as having 'limited' defence in depth, since the breaks postulated in the design phase were small, the containment capacity limited, etc.;
- failure to take seismic risk into account in the design phase;
- failure to qualify equipment for accident conditions.

The support provided by RISKAUDIT then increased and broadened considerably in scope. RISKAUDIT now offers services in the context of international projects financed by the European Commission, the EBRD[136] and the EIB[137], and also works through bilateral contracts going well beyond Eastern European countries alone. These services, which involve nuclear reactors as well as fuel cycle facilities, decommissioning, and nuclear waste management, are mainly provided by the parent institutes, IRSN[138] and GRS, with support from European safety authorities and TSOs. The type of activities performed by RISKAUDIT can be summarized as follows:

- providing technical support during the review and authorization process required to implement safety improvements on power reactors or other nuclear facilities. This type of support operates through the European TACIS and INSC programmes, in a '2 + 2' manner: on one hand, the local safety authority and its technical support teams, and on the other hand a European safety authority supported by RISKAUDIT;
- providing support with regard to regulations, organization of a safety authority, and emergency response preparedness;
- transferring knowledge and know-how (such as using simulation software for safety analyses), or sharing methods, to reinforce the capabilities of local safety organizations and develop their safety culture;
- performing safety assessments by multinational teams in compliance with internationally accepted practices;
- contributing to the harmonization of practices and approaches;
- building and maintaining an independent centre of qualified expertise.

Among the many work programmes carried out by RISKAUDIT since 1992, the following are particularly noteworthy:

- for those funded by the European Commission:
  - TACIS (Technical Assistance to the Commonwealth of Independent States and Georgia – 1992-2006),
  - PHARE[139] (1989-2006),
  - INSC (Instrument for Nuclear Safety Cooperation – 2007-2013 and then 2013-2020).

[136] European Bank for Reconstruction and Development.

[137] European Investment Bank.

[138] The headquarters of RISKAUDIT are in Fontenay-aux-Roses, France. A branch office has also been set up in Kiev, Ukraine.

[139] This acronym stands for Poland and Hungary Assistance for Restructuring their Economies, a support programme that began in 1989, but was later extended to other countries wishing to become members of the European Union: the Czech Republic, Estonia, Lithuania, Latvia, Slovakia, Slovenia, then Bulgaria and Romania.

Within the framework of these programmes, apart from work designed to improve power-reactor safety, a large part of RISKAUDIT's activities is devoted to: assessing the safety of legacy waste storage facilities, particularly on the Chernobyl power plant site and in the surrounding exclusion zone; safety assessments conducted on new facilities for the recovery, treatment, conditioning, storage and final disposal of waste; and providing assistance for the preparation of regulatory documents;

- for those financed by the EBRD:
  - providing support for decommissioning the four VVER 440/230 reactors at the Kozloduy nuclear power plant in Bulgaria, which were definitively shut down between 2002 and 2006,
  - providing assistance in the safety assessment of the new dry-storage facility for irradiated fuel at the Chernobyl power plant in Ukraine,
  - providing support for dismantling the damaged Chernobyl reactor (sarcophagus, waste treatment units).

The main beneficiaries of RISKAUDIT assistance have been Russia and Ukraine and, to a lesser extent, Bulgaria, Lithuania and Armenia.

Gradually, in the context of the European INSC programmes, RISKAUDIT's assistance has evolved into cooperation with safety authorities and expert bodies in various countries, particularly those where it has previously provided support (such as Ukraine). In addition, the INSC has extended its scope of activity to countries bordering the Mediterranean Sea, the Far East and the Americas, etc.

RISKAUDIT has carried out and continues to carry out work under bilateral agreements:

- with the Lithuanian safety authority VATESI: decommissioning of the two 1500 MWe RBMK reactors at the Ignalina plant (shut down in 2004 and 2009 respectively), in parallel with the construction of several facilities for waste treatment and storage, and dry storage of spent fuel;
- with the Bulgarian safety authority BNRA: cooperation involved reviewing the preliminary safety analysis report in 2006 for two 1000 MWe Russian VVER reactors to be built at the Belene site in northern Bulgaria. The project was abandoned in 2013;
- with the Joint Research Centre (JRC) in Petten for analyses of operating experience feedback.

The 1990s were also largely marked by the joint Franco-German project[140] that led, after seven years of discussions, to the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water

[140] The initial purpose was not to establish technical guidelines, but to prepare DFD positions on issues raised by the EPR designers.

Reactors, which served as the basis for designing the EPR. This subject will be further developed in Chapter 18.

Since 1999, three technical safety organizations – each providing support to the national safety authority – IRSN for France, GRS for Germany and Bel V (formerly AVN) for Belgium, have been involved in the EUROSAFE initiative, particularly through discussion forums aimed at sharing information and converging practices in areas relating to safety, radiation protection and security in general.

Aiming for greater commitment, however, ETSON (European Technical Safety Organisations Network), was created in 2006, bringing together European members (in 2019: IRSN, GRS, Bel V, as well as VTT [Finland], MTA EK [Hungary], ENEA [Italy], LEI [Lithuania], CVŘ [UJV] [Czech Republic], VUJE [Slovakia], JSI [Slovenia], PSI [Switzerland], RATEN ICN [Romania] and Wood [UK]), as well as three associate members from outside the European Union: SSTC NRS (Ukraine), SEC NRS (Russia) and NRA (Japan).

ETSON membership is obtained by invitation from its members and is limited to organizations that conduct safety assessments to assist their national safety authorities or that hold this function. They must display a comprehensive view of the regulatory function and conduct assessments on a regular basis, while covering a wide range of subjects. Membership is open to organizations from the European Union and the European Free Trade Association (such as Switzerland and Norway), provided they meet the membership requirements defined by the ETSON partners and specified in their statutes. Other organizations outside the above-mentioned geographical area may apply as associate members.

The purpose of ETSON is to promote the exchange of information on safety assessments, methods and research in the field of nuclear safety and security. With a view to harmonization, ETSON members prepare assessment guides, available on the website www.etson.eu. They include:

– a general document, the Safety Assessment Guide (SAG), which outlines the methodology used in Europe for safety assessments. It presents the various conditions necessary[141] to assess nuclear safety in keeping with the set objectives and applicable requirements, as well as the technical elements essential to conducting an assessment;

– a series of technical guides, called the Technical Safety Assessment Guides (TSAGs), on various topics of interest for assessors. Noteworthy subjects that have been published in guides include:

    - analysis of events and precursors to a severe accident,
    - deterministic analysis of core-melt accidents,
    - human and organizational factors in the design and modification of nuclear facilities,

[141] Independence, competence, traceability and transparency.

- studies on thermal-hydraulic transients associated with design-basis (reference) operating conditions[142].

These technical guides are prepared by working groups whose participants must have solid knowledge of the nuclear safety assessment methods implemented in their country. The purpose of these guides is to promote and disseminate best practices for the assessment of nuclear safety at European level. Each member of ETSON can thus use methods harmonized at the European level, apply them in their safety analyses and share feedback.

In 2011, ETSON also prepared a position document[143] on the safety topics to be considered in future research programmes for current and next-generation power reactors[144], with the associated priorities. These topics were addressed in the European research agendas defined by the NUGENIA[145] association created in 2011, following the reflections and work carried out within the context of the SNETP platform[146].

Lastly, European TSOs have set up training courses within the framework of a dedicated institute, ENSTTI (European Nuclear Safety Training & Tutoring Institute[147]), created in 2010. These courses aimed at promote European know-how in nuclear safety and safety assessment. ENSTTI courses were taken over by IRSN in 2020.

3.1.9. Nuclear regulator associations

In 1999, an association bringing together the heads of Western European safety authorities was created: the Western European Nuclear Regulators Association (WENRA). André-Claude Lacoste, then Director of Nuclear Facility Safety in France, was the initiator and first president. The initial aims of this association were to:

- create an organization capable of reviewing the level of nuclear safety achieved in the candidate countries for accession to the European Union. WENRA's initial work thus led in 2000 to an assessment of nuclear safety control as organized in Bulgaria, the Czech Republic, Hungary, Lithuania, Romania, Slovakia and Slovenia, and a safety assessment of the power generating reactors in these countries;
- develop a common approach to nuclear safety.

[142] This concept is explained in Chapter 8.

[143] Position Paper of the Technical Safety Organisations: Research Needs in Nuclear Safety for GEN 2 and GEN 3 NPPs – ETSON/2011-001, October 2011.

[144] See Chapter 18.

[145] NUclear GENeration II & III Alliance (international association dedicated to the safety of Generation II and III reactors).

[146] Sustainable Nuclear Energy Technology Platform.

[147] Training and tutoring organization specialized in nuclear safety. It was a European economic interest grouping, EEIG.

Composed of ten members when it was created, WENRA now has[148] 18 members and 13 observers (although the name remains the same, many of these countries are not from Western Europe). Beyond the development of harmonized approaches, WENRA can express its opinion on regulatory issues or other safety aspects.

Several working groups, usually attended by representatives of technical support organizations, including IRSN, have issued reference documents that take into account IAEA standards and best practices in the relevant countries.

For power reactors, WENRA established 'reference levels'[149] for reactors in operation and safety objectives for future reactors. The reference levels include regulatory and technical aspects. The commitment made by WENRA members was to introduce the notion of reference levels into their regulations by 2017 and ensure their implementation. In France, this led to the publication of documents such as the ASN Guide No. 22 mentioned in Chapter 2.

In July 2007, a European Commission decision created a European group called the European Nuclear Safety Regulators Group, or ENSREG. It includes representatives of safety authorities from across the European Union[150], as well as representatives of the European Commission. Switzerland, Norway and the IAEA also have observer status. This group, whose mission is to advise the European Commission, aims in a very general way to reach a common understanding of safety issues and to establish the conditions for continuous improvement of safety, while also improving transparency.

ENSREG advises and assists the European Commission either at the request of the Commission or on its own initiative. It is obliged to consult stakeholders and the relevant public audience in an open and transparent manner. It must submit regular progress reports to the European Commission, including recommendations as appropriate, to be forwarded to the European Parliament and the Council.

Based on positions defined by the Council of the European Union, ENSREG initiated discussions on safety, radioactive waste and spent fuel management, and transparency in the nuclear sector at European level. This work contributed to the adoption of the Nuclear Safety Directive 2009/71/EURATOM of 25 June 2009, establishing a Community framework for nuclear safety in nuclear facilities, as amended by Directive 2014/87/EU of 8 July 2014, both referred to in Chapter 2.

The above shows the growing role of the European Commission, which initially had little power in terms of assessment, but financial resources for research and development work (through Framework Programmes).

[148] As at January 2019.

[149] These 'reference levels' are discussed in Chapter 6.

[150] France has two representatives in this organization: the ASN Chairman and a representative of the DGEC.

3.2. The social dimension

3.2.1. Introduction – the context in France

The growing involvement of civil society in France on issues relating to the safety of nuclear activities and facilities is developed in Section 2.3. Significant milestones are indicated, from the formation of non-profit organizations to the recognition by public authorities of the importance of civil society, with a description of its involvement and concrete initiatives, especially in the context of local information commissions (CLIs, active at all French nuclear power plants) and the National Association of Local Information Committees and Commissions (ANCCLI).

To illustrate the involvement of civil society, a few examples of initiatives and issues raised by civil society concerning reactor safety in French nuclear power plants are described below in chronological order. The parts of this book dealing with topics related to these issues are mentioned and will help to enlighten the reader.

3.2.2. Examples of initiatives and issues raised concerning reactor safety in the French nuclear power plant fleet

In 1989, the local government authority (*Conseil général*) of the Upper Rhine set up a group of experts to assess the results of the first ten-yearly periodic review of Unit 1 at the Fessenheim nuclear power plant, which started up[151] in 1977. The members of this group were selected to ensure a broad diversity of expertise. It included scientists and members of non-profit organizations from Germany, France and Belgium. The group was also to benefit from the expertise of scientists from Strasbourg who had followed operation of the reactor from startup, along with a study undertaken on the environment surrounding the Fessenheim plant.

At the end of their mission, while experts regretted a lack of time and means, as well as the intermittent nature of the information they had received, three distinct subjects seemed to them to deserve special attention: checks performed before restarting the reactor, worker protection, and ‘beyond-design-basis’ accidents (i.e. accidents studied, even though their characteristics are not included in the reactor design basis – see chapters 8 and 13). They expressed concern about the postponement of certain safety improvements and issued criticism regarding radioecology around the site, also deploring that they had not received information on the substances discharged from the facility. Their report exposed debates that had taken place within the group itself. They considered that special attention should be given to protecting the facility from aeroplane crashes and core-melt accident scenarios. Regarding core melting, hydrogen risks were a subject of debate[152].

[151] This refers to the moment when it was connected to the power grid. Actual commissioning took place in 1978.

[152] They were based mainly on experiments carried out in the PHEBUS research reactor.

Later, during analysis of the generic aspects of the safety review for the third ten-yearly inspection outage for 900 MWe reactors, ANCCLI experts and CLI representatives from nuclear power plants at Fessenheim, Gravelines, Blayais and Dampierre-en-Burly asked to hold discussions with the safety organizations. These experts met on five occasions between December 2009 and November 2010. The topics covered both internal and external hazards (subjects treated at greater length in chapters 11 and 12, such as fire, floods, earthquakes, aeroplane crashes, etc.), core-melt accidents (examined in Chapter 17) and equipment ageing (in Chapter 27). The CLIs were particularly interested in knowing how changes in the industrial environment of a basic nuclear installation were generally taken into account, as was the case with the project to build a liquefied natural gas (LNG) terminal near the Gravelines nuclear power plant (a subject discussed in Section 12.9). CLIs approached other subjects not specific to periodic reviews that they found worthy of attention: human and organizational aspects, such as skills management and oversight of subcontracted activities (see Chapter 25), and analysis of 'significant events' (a concept explained in Chapter 21). CLIs also emphasized their interest in being allowed to consult the responses given by operators when questioned by ASN on given subjects.

At the same time, the CLIS[153] at Fessenheim asked the Scientific Group for Information on Nuclear Energy (*Groupement de scientifiques pour l'information sur l'énergie nucléaire*, GSIEN) for an assessment of the third ten-yearly periodic review of the reactors at the Fessenheim nuclear power plant[154]. This study suggested areas for improvement concerning maintenance, setting up construction sites and worker training. The CLIS also raised concerns on several other points: the strength of the basemat in the event of a core-melt accident (these basemats have been thickened – see sections 17.1.5 and 30.4.5), waste with no disposal solutions, increased tritium discharges to the environment correlated with the changeover to Cyclades fuel management (fuel management is presented in the Focus feature in the introduction to Chapter 28), leading to greater use of boron as a neutron absorber, and the combined use of equipment designed in the 1960s and 1970s with other more recent equipment.

Following the 2011 Fukushima Daiichi NPP accident, and as further developed in Section 36.6 of this book, public authorities asked operators to conduct Complementary Safety Assessments (CSAs) in compliance with specifications that had been extended to include a section on issues relative to subcontracting, subsequent to discussions with the HCTISN. In this context, ANCCLI and the CLIs sought to become more involved in the safety analysis of facilities, particularly nuclear reactors.

Dialogue began in September 2011 among all interested parties, before the meetings of the advisory committees responsible for giving an opinion on the complementary

[153] Local Information and Oversight Commission for the Fessenheim nuclear power plant.

[154] GSIEN experts have had access to documents written by EDF, IRSN and ASN subsequent to an agreement among the various parties. They produced the *Rapport sur la visite décennale n° 3 du réacteur 1 du CNPE de Fessenheim* (Report on the Third Ten-yearly Periodic Review of Unit 1 at the Fessenheim Nuclear Power Plant), GSIEN, June 2010, https://www.anccli.org/wp-content/uploads/2014/06/Rapport-final-1-VD3-FSH-1.pdf.

safety assessments carried out by operators. All the documents produced – operator reports, IRSN reports, advisory committee opinions, reports and decisions issued by ASN – for the first time on this type of subject matter, were made public immediately after their release (on the ASN and IRSN websites). These documents and the associated discussions allowed the CLIs, non-profit organizations and non-institutional experts to conduct and present their own analysis of the subject at meetings (Figure 3.4 illustrates one presentation). In this manner, several non-institutional experts conducted critical analyses of the assessments conducted by the operators. Among the more noteworthy were the analysis conducted by the Institute for Energy and Environmental Research (IEER) and WISE-Paris for Greenpeace[155], and the study carried out by GSIEN for ANCCLI[156]. The IEER report, for example, pointed out that the proposed approach for checking facility compliance with applicable requirements appeared insufficient to report on the true state of facilities, citing a certain number of 'generic deviations'[157] (see Chapter 29). The GSIEN report indicated that the subject on subcontracting was not dealt with appropriately to address emergency response situations. It raised the question of what action should be taken so that subcontractors present on site when an accident occurs can be included in the company's in-house teams, after receiving appropriate training so that they can respond effectively and stay informed of any possible risks.

The local information commissions in the Manche area (in northwest France, in Normandy) showed a particular interest in this subject by setting up a working group bringing together several local information commissions to form the 'Inter-CLI' group. In 2012, after analysing the available documents, the group prepared a survey containing nearly 200 questions relating to facility safety, emergency response, and population and environmental monitoring. They then interviewed various entities concerned, including EDF, CHSCTs[158], ASN, IRSN and others. At the end of 2013, they issued a white paper[159] compiling all the responses received, as well as a summary analysis of their results.

[155] *Sûreté nucléaire en France post-Fukushima : Analyse critique des évaluations complémentaires de sûreté (ECS) menées sur les installations nucléaires françaises après Fukushima* (Nuclear Safety in Post-Fukushima France: Critical Analysis of Complementary Safety Assessments on French Nuclear Facilities after Fukushima), A. Makhijani, Institute for Energy and Environmental Research (IEER) and Y. Marignac, WISE-Paris (World Information Service on Energy-Paris), February 2012.

[156] *Analyse et commentaire des rapports d'évaluation complémentaire de la sûreté des installations nucléaires au regard de l'accident de Fukushima* (Analysis and Comments on Complementary Safety Assessments of Nuclear Facilities Following the Fukushima Accident), M. and R. Sené, GSIEN, November 2011.

[157] Deviations affecting or likely to affect several reactors in the nuclear power plant fleet.

[158] Health, safety and working conditions committees (CHSCT) from Areva (including subcontractor representatives) and EDF.

[159] *Livre blanc sur la sûreté des installations nucléaires civiles de la Manche post-Fukushima* (White Paper on the Safety of Civil Nuclear Facilities in the Manche Area after Fukushima), Inter-CLI, Manche Local Information Commissions (December 2013).

Figure 3.4. Picture taken during a seminar held by ANCCLI and IRSN in June 2013, during which two representatives of Greenpeace presented an analysis of the complementary safety assessments conducted following the Fukushima Daiichi nuclear power plant accident (covered in Section 36.6). Grégoire Maisonneuve/IRSN Media Library.

In the case of reactors, for example, the white paper raised the question of the possibility of replacing the use of zirconium alloy in fuel cladding with another material, as its oxidation is the primary cause of hydrogen formation. Research actions initiated by fuel assembly manufacturers, cited at the end of Section 28.2, relate in particular to this subject.

Encouraged by the interest that CLI members have shown in safety issues since 2011 and given the perspective of reactor operation being extended beyond 40 years, a series of technical discussions[160], engaged in 2014, has moved forward gradually with regard to the periodic review associated with the fourth ten-yearly outage of 900 MWe reactors. This dialogue provides CLIs the opportunity to examine in greater depth their issues of concern, such as controlling ageing of the reactor vessel and containment, equipment conformity, naturally occurring risks (hazards), risks associated with spent fuel storage pools, core-melt accidents, etc. In addition, a national consultation[161], directed by the HCTISN, was conducted to achieve greater public participation in this review, where the issues at stake are quite particular.

From all the discussions and debates already held, many questions have emerged from CLI members, for example on the confinement and protection of spent fuel storage pools (a certain number of risks related to the pools and the accident situations

[160] Five meetings were held in Paris between 2014 and 2016, a seminar in Valencia in October 2016, and three new meetings in Paris between 2017 and 2018.

[161] Consultation on the safety upgrades of the 900 MWe reactors on the occasion of their fourth ten-yearly periodic review, from September 2018 to March 2019; see the website https://concertation.suretenucleaire.fr.

taken into account are developed in Chapter 15). The impact of climate change on safety also raises many questions, including the measures that would be taken to anticipate or manage situations such as a decrease in the flow of a river used as a heat sink, or on the contrary a rise in sea level for plants located on the sea shore (risks covered in sections 12.4 and 12.6). Finally, the ability of industry to perform the planned modifications to approach the safety level of an EPR-type reactor is frequently questioned.

Lastly, in view of the questions raised by civil society, the handling of the anomalies discovered in the upper and lower heads of the Flamanville 3 EPR vessel also led to technical dialogues. EDF, Areva NP, ANCCLI, the Flamanville CLI, ASN and IRSN held several meetings beginning in December 2015. Going beyond simply understanding the technical files under investigation, they questioned, in particular, whether the fundamental principles of defence in depth were being applied appropriately (taking into account the fact that the vessel is a component for which rupture is excluded by a high level of prevention – a notion discussed in greater detail in Section 8.2.2), as well as the governance of safety in general.

These dialogues with civil society and the public give safety organizations[162] material for discussing issues raised by the public.

[162] For example, IRSN addressed a number of issues arising from technical dialogues with society in its opinions on the fourth ten-yearly periodic review of the 900 MWe reactors (for example, in those on accident studies, internal and external hazards, equipment compliance, organization of EDF and probabilistic safety assessments), summarized its responses on the issues addressed in a ‘frequently asked questions’ section updated to reflect the new opinions issued and produced several explanatory videos, some of which capture the dialogue with ANCCLI. See the IRSN knowledge bases devoted to the fourth ten-yearly periodic review of 900 MWe reactors, which can be consulted at: https://www.irsn.fr/FR/connaissances/Installations_nucleaires/Les-centrales-nucleaires/visites-decennales/Reexamen-900/Pages/0-Sommaire-quatrieme-reexamen-reacteurs-900-MWe.aspx#.

Chapter 4
Nuclear Reactors: Complex Sociotechnical Systems – the Importance of Human and Organizational Factors

Before going into further detail on safety issues specific to pressurized water reactors in the French nuclear power plant fleet, it is essential to emphasize the important role of not only technical aspects, but also the **human and organizational factors** involved in managing the risks featured in these facilities.

Analysis of incidents and accidents (in all fields of activity, not just the nuclear industry) shows that they are most often the result of a combination of failures and deficiencies involving equipment, organizations and people.

It is not enough to consider only the technical aspects of the design and operation of nuclear facilities: people also contribute to the initiation and development of incidents (by the very fact that they design, build and operate nuclear facilities), but they also have a positive contribution to make (for example, by correctly achieving 'recovery' from abnormal situations that occur during facility operation) – which is possible when appropriate organization and procedures have been implemented to control facility operations.

The notion of 'human and organizational factors' (HOFs) refers to the factors that influence human activity and the way in which sociotechnical systems[163] function. This includes factors such as organization, skills, technical resources, procedures, group performance and the physical work environment. The study of these factors is a relatively recent discipline that has evolved with the technological changes of the twentieth century. It has taken on greater importance in organizations responsible for high-risk facilities, as they play a decisive role in preventing or contributing to many industrial accidents. A strong assumption underlying the attention and resources devoted to the analysis of human and organizational factors (validated by experience) is that it is possible to identify preconditions or deviations in a sociotechnical system that may result in an undesirable event, which may therefore be prevented through appropriate engineering of human and organizational factors. Through a better understanding of human activity, it is thus possible to determine and create conditions that will drive people and organizations to make positive contributions to facility operation[164]: this begins with the choice of facility design options and, of course, continues during design studies, then in the definition of operating rules and procedures, and finally throughout facility operation and decommissioning.

4.1. The introduction of human and organizational factors in the field of nuclear power reactors and lessons learned from the Three Mile Island nuclear power plant accident

When the first units of the French nuclear power plant fleet[165] were commissioned in the 1970s, emphasis was placed on the technical reliability of the facilities, which relied mainly on the quality of their design, keeping operational equipment continuously in compliance with applicable requirements, and having pre-defined operating procedures, both for normal operating situations and for a certain number of abnormal situations considered plausible. In addition, command and control actions were automated, particularly to reduce the possibility of human error. The combination of equipment and human failures, however, were not examined systematically.

The importance attached to human and organizational factors has gradually increased, first through the analysis of events involving these factors, allowing lessons to be learned to prevent their recurrence, and then mainly after the accident in Unit 2 at the Three Mile Island (TMI-2) nuclear power plant in March 1979 in the USA.

[163] Systems that have many interacting technical, human, organizational and social components.

[164] For more information, see F. Daniellou, M. Simard and I. Boissières, *Facteurs humains et organisationnels de la sécurité industrielle: un état de l'art* (Human and Organizational Factors in Industrial Safety: the State of the Art), *Les Cahiers de la sécurité industrielle*, (Toulouse, France: Fondation pour une culture de sécurité industrielle, 2010). See: https://www.foncsi.org/fr/publications/cahiers-securite-industrielle/human-organizational-factors-safety/CSI-HOFS.pdf.

[165] Various parts of this chapter have been taken from EDF's *Mémento Sûreté nucléaire en exploitation* (Memento on Operational Nuclear Safety), 2016.

Analysis of the accident from the point of view of human and organizational factors led to changes and improvements concerning mainly human-machine interfaces, organization (especially in the control room operating crew, reorganized so that facility monitoring was backed up by a safety engineer), sharing feedback, and control procedures in incident and accident situations (transition from an 'event-driven' to 'state-oriented' approach), described in detail in chapters 32 and 33.

4.2. The accident at the Chernobyl nuclear power plant and the concept of 'safety culture'

While the TMI-2 accident raised questions about workstations, including ergonomic aspects such as defects in the human-machine interface and cognitive aspects such as a misinterpretation of the state of the facility, the accident at the Chernobyl nuclear power plant, examined in Chapter 34, raised other questions concerning collective and organizational aspects, as the accident sequence involved intentional non-compliant actions and overriding protective functions to carry out a scheduled low-power safety test 'at all costs'. Among other things, analysis of the accident revealed shortcomings concerning management, control of activities, application of rules and procedures and the priority that must be given to safety and operator training. The accident thus resulted in considering the human role in risk management, no longer solely from a behaviourist angle focused on reducing individual errors, but from a broader perspective taking into account the characteristics and dynamics of a complex sociotechnical system as a whole.

In terms of organizational factors, research[166] on High-Reliability Organizations (HRO) since the 1980s has provided methodologically useful insights for analysis of these factors in the design and operation of nuclear power plants. Based on the findings of organizations responsible for 'at-risk' facilities operated in a safe and reliable manner, this work has highlighted keys to success such as:

- agreement by all members of the organization on targeted goals, especially when making decisions,
- built-in redundancies (checks, decision circuits, communication channels),
- a balance between centralization and decentralization,
- continuous education and training,
- giving attention to the risk of failure in human activities, not just success,
- asking managers to direct their attention to daily activities and contingencies,
- delegating decisions to the most competent people or those closest to the field,
- being wary of simplified interpretations of complex systems,

[166] This research was carried out at the University of California at Berkeley. Readers may also wish to consult M. Bourrier, *Organiser la fiabilité* (Organizing Reliability), *Éditions L'Harmattan*, 2001), as well as K. Weick and K. Sutcliffe, Managing the Unexpected, Resilient Performance in an Age of Uncertainty (Jossey Bass, 2007).

– providing resources and processes to promote adaptation ('commitment to resilience'), in addition to risk prediction approaches.

In parallel, studies on the root causes of accidents, conducted by English-speaking and French researchers (in particular from EDF and IRSN), identified[167] generic and recurring organizational factors of failure, such as:

– pressure applied to meet production targets,

– organizational complexity,

– defective reporting in risk analyses and operating experience feedback,

– shortcomings in workforce and skills management,

– inadequate requirements issued by regulatory bodies, etc.

Lessons learned from the Chernobyl accident made a significant contribution to the development of 'safety culture' as a concept, which was widely promoted in response to this accident. In 1991, five years after the Chernobyl accident, the INSAG-4 report was published (by the IAEA). It explains the concept (see the Focus feature below) which involves not only nuclear facility operators, but also designers and manufacturers, as well as safety organizations (and even government).

#FOCUS

The Safety Culture concept

As indicated above, the concept of safety culture emerged from discussions that began after the accident on 26 April 1986 at the Chernobyl nuclear power plant. 'Post-Chernobyl' discussions argued for a more international vision of nuclear safety and were embodied in reports by the International Nuclear Safety Advisory Group (INSAG), created by the IAEA shortly after the accident. The Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident (INSAG-1[168]) published in September 1986 refers to the concept of safety culture, which was developed further in 1991 in the report entitled Safety Culture (INSAG-4). Safety culture is defined in the report as "the set of

[167] On this subject, see the following articles in *Techniques de l'ingénieur*: J-M. Rousseau and A. Largier, *Industries à risques: conduire un diagnostic organisationnel par la recherche de facteurs pathogènes* (At-risk Industries: Conducting Organizational Diagnostics by Searching for Pathogenic Factors), AG 1 576-1, 2008, and M. Llory and Y. Dien, *Systèmes complexes à risques – Analyse organisationnelle de la sécurité* (At-risk Complex Systems – Organizational Analysis of Safety), AG 1 577-1, 2010. See also the article by N. Dechy, Y. Dien and M. Llory, *Pour une culture des accidents au service de la sécurité industrielle* (For a Culture of Accidents to Serve Industrial Safety), *17e congrès Lambda Mu de Maîtrise des risques et de sûreté de fonctionnement* (17th Lambda Mu Conference on Risk and Operational Safety Management), October 2010, La Rochelle, France.

[168] See INSAG-7 (1992) for the updated report.

characteristics and attitudes in organizations and individuals which establishes that […] safety issues receive the attention warranted by their significance." Safety culture assumes that a questioning, prudent and rigorous attitude and good communication between individuals are encouraged within the organization. It requires a strong commitment from line and facility managers.

Three other INSAG reports are worthy of mention at this point:

- Management of Operational Safety in Nuclear Power Plants (INSAG-13, 1999). This report addresses the aspects of 'safety management' that are important in promoting safety culture, along with recommendations and good practices. It contains recommendations on maintaining appropriate safety management during periods of organizational change, monitoring safety performance and early identification of declining performance before it has a significant impact on safety;
- Key Practical Issues in Strengthening Safety Culture (INSAG-15, 2002). This report raises a certain number of questions that need to be asked during self-assessment of an organization's safety culture and addresses key issues such as: the importance of good communication and making sure that safety issues are understood correctly, especially with regard to procedures, which must be comprehended by the users themselves; fostering a 'reporting culture', focusing on near misses and the possible ensuing deviations ('to tolerate is to validate'[169]); and an organization's ability to challenge its performance at all levels (to become a 'learning organization');
- Managing Change in the Nuclear Industry: the Effects on Safety (INSAG-18, 2003). This report addresses a number of topics concerning the consequences of change on organizations and people in the nuclear context (striving to improve competitiveness, increased safety requirements and other issues), which can affect safety if they are not sufficiently well integrated and managed.

In a more recent report[170], the IAEA defined a framework and requirements pertinent to safety management and an integrated management system in a systemic approach that takes into account interactions between technical, human and organizational factors, in order to foster a 'strong safety culture'.

The safety culture concept has also been widely used in other fields with high-risk activities such as aeronautics, the chemical and oil industries and medicine. However, while the concept may seem simple to understand, it does not provide a sufficient answer to all questions concerning how people and organizations

[169] See the work of the American sociologist D. Vaughan on the Challenger accident: The Challenger Launch Decision, Risky Technology, Culture and Deviance at NASA (1996). It shows that what in hindsight appears to be a series of clearly identifiable errors is actually a series of decisions and interpretations that are perfectly understandable in the context in which they were made, but which are in fact slight deviations from design limits that lead imperceptibly to the normalization of deviance.

[170] Leadership and Management for Safety, IAEA Safety Standards, No. GSR Part 2, 2016.

contribute to safety. For example, questions remain about the conditions, procedures and limits of 'engineering' a safety culture. While the implementation of organizational and management measures can contribute to the development of a safety culture, the way in which these measures combine their effects to positively or negatively influence safety culture is still insufficiently ascertained.

In March 2002, an incident (classified as Level 3 on the International Nuclear Event Scale), sometimes referred to as a near-accident, occurred at the Davis-Besse nuclear power plant in Ohio, in the USA. The plant features a 900 MWe pressurized water reactor[171]. This incident has influenced discussions and concerns about human and organizational factors within the nuclear energy industry, including at EDF[172]. The event, which resulted in a loss of leaktightness in the reactor coolant system at the reactor vessel head, is described later (Section 27.2.2.9). Analyses suggested that the incident was indicative of significant problems in the safety culture and inadequate oversight on the part of authorities. In particular, the following were highlighted:

- failure to take into account precursors which were detected beginning in 1996, including traces of boron on certain items of equipment,
- insufficiently developed event analyses, which only took limited account of international operating experience,
- lack of commitment to safety management displayed by plant executives, preoccupied by prevailing production issues,
- inadequate oversight by authorities.

In some respects, this near-accident could be compared to the Challenger and Columbia shuttle accidents, where analyses also revealed a failure to take into account precursors[173].

At EDF, the event at the Davis-Besse nuclear power plant resulted in various measures[174], including:

- the preparation of decision-making guides to adequately incorporate safety requirements when setting power generation objectives,
- the implementation of 'safety management' consistent with international practices in light of the INSAG-13, INSAG-15 and INSAG-18 reports presented in the previous Focus feature,

[171] The reactor was manufactured by Babcock & Wilcox.

[172] See *Mémento sûreté nucléaire en exploitation* (Memento on Operational Nuclear Safety), EDF (2016).

[173] See the work of D. Vaughan cited above, as well as the report by the U.S. Department of Energy, Action-Plan on Lessons Learned from the Columbia Space Shuttle Accident and Davis-Besse Reactor Pressure Vessel Head Corrosion Event, 2005.

[174] EDF, Memento quoted above.

– adoption of an operating experience feedback procedure that takes into account precursors, international feedback and the search for the root causes of events.

As demonstrated by the near accident at the Davis-Besse nuclear power plant, safety culture must manifest itself regularly when important decisions are to be taken and safety has top priority. Faced with high staff turnover, for several years EDF has adopted an approach aimed at reinforcing safety culture. A guide was distributed to nuclear power plants to build a shared notion of safety culture among members of personnel. With this in mind, EDF deploys training, daily communication through various channels and self-positioning in operational units, so that everyone is aware of the need to step back and take a look at their own practices.

In addition, given the high volume of subcontracted maintenance operations (considered in Chapter 25), the operator is taking appropriate measures to ensure that safety culture is integrated into subcontractor practices.

4.3. The Fukushima Daiichi nuclear power plant accident: the social dimension and the concept of organization 'resilience'

More recently, the 2011 Fukushima Daiichi nuclear power plant accident revealed the importance of the social dimension in risk governance in general, an aspect underscored by the commission of inquiry in their report to the Japanese Diet after the accident.

Following the accident, studies and research were initiated[175] on nuclear risk governance and emergency response, addressing not only organizational factors but also cultural and social-historical factors.

Certain lessons from the Fukushima Daiichi nuclear power plant accident and its management also indicate the need to change how the role of people and organizations is perceived in risk management, an idea that has gradually emerged since the 1990s. This evolution is discussed below.

4.4. Changes in the perception of the role of people in achieving a high level of reliability in complex sociotechnical systems

After more than thirty years of experience in taking human and organizational factors into account in nuclear safety, the knowledge acquired shows that the reality of operation is far from simple and that people play a decisive role in keeping facilities

[175] See J. Couturier and M. Schwarz, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2018, Chapter 11. In 2012, it was in this field, which falls within the human and social sciences, that IRSN and other partners decided to undertake further studies, within the framework of the AGORAS project funded by the French National Research Agency (*Agence nationale de la recherche*, ANR).

operating correctly. Through their competence and skills, they are able to cope with and adapt to the variety of situations they encounter in their daily work: unavailable equipment, non-compliant parts, incomplete description of what needs to be done and how to do it as indicated in procedures, instructions and work process documents, changing working conditions, varying levels of staff expertise, etc.

The ability to adapt involves actions that people can take outside of the procedure planned to ensure safe facility operation; however, the appropriate conditions must exist to allow them to cope and make the necessary adjustments. The Fukushima Daiichi nuclear power plant accident demonstrated the ability of plant operators to adapt and invent solutions under very difficult working conditions in order to deal with an extreme situation for which they were unprepared.

The following questions therefore arise: are the conditions met for personnel to carry out their activities as well as possible and use their competence and skills, including detecting system deviations and recovering from degraded or even critical situations? Are individuals and work crews able to cope with unplanned situations using the resources at their disposal? Does management make decisions that sufficiently facilitate risk control in unplanned situations?

Taking into account human and organizational factors must therefore have a twofold objective for the operator:

- promote the ability of personnel to detect technical anomalies, manage contingencies and reduce the possibility of inappropriate human action as much as possible;
- promote the ability of people to adapt to new problems and to cope with unexpected situations[176] so that the group is able to control the situation.

Taking into account human and organizational factors[177] must therefore lead to identifying and evaluating the conditions required to achieve these two objectives by

[176] For further information, see B. Bernard, *Comprendre les facteurs humains et organisationnels – Sûreté nucléaire et organisations à risques* (Understanding Human and Organizational Factors – Nuclear Safety and At-Risk Organizations), EDP Sciences (2014), as well as the report of the Steering Committee for Human, Social and Organizational Factors (COFSOH), *Développer la sécurité: Synthèse des travaux du groupe de travail D* (Developing Safety: Summarized Results of Working Group D), September 2019, available in French on the ASN website. The same duality between expectations and 'resilience' is found in the distinction between 'regulated' safety and 'managed' safety:

- 'regulated' safety: consists in avoiding predictable failures by relying on formal procedures, rules, automation, protective measures and equipment as well as management staff that ensures compliance with rules;
- 'managed' safety: represents the ability of the organization and its actors to perceive unexpected situations and to respond to them in an appropriate manner. It is based on human expertise, the quality of initiatives, the manner in which groups and organizations function, and management principles and design processes that take into account real situations.

[177] An approach described as 'integrated and systemic'.

analysing the technical, human and organizational dimensions of the sociotechnical system as a whole, as well as the interdependence between these three dimensions.

In the early 1980s, in designing the N4 reactor series, EDF chose to implement computerized instructions for operation in normal, incident and accident situations (which guided design of the control room for these reactors). This led EDF and IRSN to question whether 'step-by-step' guidance of operators using instructions of this type was appropriate, leading to further research on this matter[178]. Various studies, including fields other than nuclear power generation, had in fact shown that the field operator must be actively involved in operation for guidance to be effective. Consequently, guidance must not discourage operators from 'keeping a certain distance' with regard to recommendations given in procedures. This condition favours the positive role of the operator, for example, in situations where it is difficult to follow the order of actions prescribed by instructions when an action is perceived as urgent. The studies therefore led designers to make certain improvements, such as:

- technical enhancements, where the control system gives the operator the option to deviate from the prescribed path at any point in the computerized instructions whenever the recommended actions are not in phase with the process kinetics,
- organizational benefits, by allowing an operator to take this type of decision only after consulting with the operating crew and receiving approval from the shift manager.

The Fukushima Daiichi nuclear power plant accident also led to questioning the robustness of the emergency response organizations called on to manage an extreme situation such as the one that led to this accident. Studies of emergency situations related to major events or disasters highlight the state of 'breakdown' caused by the suddenness and scale of the resulting disorder, which submerges the planned human and organizational capabilities. These situations take place in the context of an emergency where it is necessary to coordinate a large number of responders who are exposed to hazards and malfunctions caused by the accident. They find themselves unable to accomplish their mission and fulfil the responsibilities formally planned to respond to the accident and manage the emergency situation. The questioning concerns matters such as the size of the workforce required, the training and preparation of personnel for these situations, the ability to mobilize plant personnel and subcontractors, the feasibility of taking action locally in difficult or even hostile conditions. These are issues that were addressed in the complementary safety assessments conducted in the aftermath of the Fukushima Daiichi nuclear power plant accident, which, in France, led to the implementation of a 'hardened safety core' of robust equipment and the Nuclear Rapid Response Force, described in further detail in Chapter 36.

[178] J. Couturier and M. Schwarz, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2018, Section 11.2.2-B.

4.5. Main topics studied in the development of resources and skills pertaining to human and organizational factors

4.5.1. Resources and skills

Internationally, initial research conducted in the 1970s aimed to gain a better understanding of human 'functioning' and its influence on the performance of nuclear power plant personnel not only during operations in the control room, but also during all tasks and activities (tests, maintenance, in-service inspections, etc.) performed outside the control room and which may be important to nuclear safety. The scope of research was subsequently extended to understand and assess organizational, cultural and societal factors. The Nuclear Energy Agency of the Organisation for Economic Co-operation and Development (OECD/NEA) issued numerous reports demonstrating the international community's interest in human and organizational factors[179] immediately following the accident at the Three Mile Island nuclear power plant.

Over time, human and organizational factors have become increasingly important in international research. Organizations such as the IAEA and NEA are valuable forums for exchanging ideas. Nonetheless, while safety organizations in a number of countries have acquired solid experience, the global situation remains disparate. The field of human and organizational factors is an important area of development for countries that do not yet have sufficient experience and skills to conduct studies, research, assessments or inspection programmes in human and organizational factors.

This is why, in 2014, the IAEA, with the collaboration of experts from various countries, launched a four-year programme to assist safety organizations in setting up and reinforcing their action in the field of human and organizational factors. The programme was completed in 2018 with the publication of a report devoted solely to this subject to encourage the development and implementation of inspection and assessment programmes in human and organizational factors[180].

In France, beginning in the late 1970s, both EDF and IPSN acquired specific skills in human and organizational factors, which were further enhanced in the 1980s. Research units were then set up to develop the knowledge required for safety analysis, to deal with new issues (new technologies and fields) and explore societal issues relating to the governance of nuclear risks in terms of organizational as well as cultural factors[181].

[179] D. Tasset, A. Frischknecht, G. Lamarre, B. Gil-Montes, International Collaboration in Nuclear Safety – Contribution of the NEA/CSNI Working Group on Human Organizational Factors, paper presented at the ANS 8th International Conference on Nuclear Power Plant Instrumentation, Control and Human-Machine Interface Technology, San Diego, USA, 22-27 July 2012.

[180] Regulatory Oversight of Human and Organizational Factors for Safety of Nuclear Installations (IAEA-TECDOC-1846) serves as a guide for this effort.

[181] See J. Couturier and M. Schwarz, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2018, Chapter 11.

The study of organizational and human dimensions is based on multidisciplinary approaches that use knowledge, models and techniques from human and social sciences[182] to understand the 'real functioning'[183] of sociotechnical systems. These approaches apply in particular to facility design and normal operating phases, as well as operating event feedback and the facility decommissioning phase.

The study of human and organizational factors generally requires field observations (interviews with personnel, observations of work sites or work situations, for example, during 'safety sensitive' activities and others). When these analyses are carried out in the context of safety assessments, they require the implementation of protocols between IRSN and the operator concerned[184]. The study can also be based on simulations such as those conducted at the Halden Man-Machine Laboratory[185] (HAMMLAB)[186] of the research reactor in Halden, Norway, as part of the international HALDEN Reactor Project.

The type and quality of data collected through field observations and simulations are essential to producing valid results. Interviews with actors make it possible to collect not only facts but also subjective data (opinions, feelings and perceptions). The interviews are conducted with several people and cross-referenced with objective data (such as organization notes, changes in the physical parameters of a system or notes and photographs of observations). Establishing the 'sum' of the subjective information collected and objectifying[187] this data results in a fairly accurate picture of reality.

In the early 1990s, EDF considered that in order to make progress in event analysis, specialists in human and organizational factors should be placed inside nuclear power plants in service to observe field operations as closely as possible. As a result, since 1995, each plant has a specialist designated as the Human Factors Consultant. EDF's corporate headquarters oversees this network of consultants to consolidate and capitalize on action taken and exchange information on practices.

Starting in 2005, EDF set up a network of specialists in its engineering centres to analyse human, social and organizational impacts – an approach explained in

[182] These sciences aim to explain reality and its phenomena through knowledge of the corresponding causes, 'laws' and 'models': the existence of regular patterns even for apparently very individual behaviour, occurrence of these patterns in organizations (individuals with the same profile, placed in the same situation, will have similar behaviour and similar action strategies).

[183] The concept of 'real functioning' refers to practices implemented in the field and differs from what is planned in procedures and formalized in operating documentation.

[184] The purpose of these protocols is to specify the conditions for interviews and observations, in particular to protect the confidentiality of statements made and the anonymity of the people interviewed.

[185] A laboratory specializing in human-machine interfaces.

[186] See J. Couturier and M. Schwarz, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2018, Chapter 11.

[187] See IRSN DSR Report 438, *Les facteurs organisationnels et humains de la gestion des risques: idées reçues, idées déçues* (Human and Organizational Factors in Risk Management: Preconceived Ideas and Disappointment), released in 2011 and available in French on the IRSN website.

Section 16.2.2 – to develop the process of considering human and organizational aspects when making technical and documentation changes.

EDF has also taken action to reduce the number of events involving human failures occurring in its fleet of nuclear reactors by relying on the people competent in human and organizational factors available both at corporate level and at nuclear power plant sites. Since 2006, it has taken measures at all plants to improve the reliability of human action in order to help each professional 'get it right the first time', based on internationally recognized standard practices to ensure the reliability of work tasks: pre-job briefing, the 'one-minute pause', special checking procedures (self-checks or cross-checks), 'secure' communication[188] and debriefing.

4.5.2. Main topics studied

Beginning in the early 1980s, following the accident at the Three Mile Island nuclear power plant, experts and researchers at EDF and IPSN, particularly in ergonomics, contributed to studies on control room activities and participated in the design project for the computerized control room of the N4 plant series. The study of human and organizational factors at the design stage continued during EPR design[189]. The subjects dealt with included the integration of human and organizational factors in design methodology, human-machine interfaces, control systems provided for control room operators (mentioned earlier), the organization of operating crews, and operator action in the field. Starting in the 2000s, human and organizational factors were also taken into account extensively when designing and implementing physical and organizational changes in nuclear power plants in service. Taking into account human and organizational factors when designing new facilities or making changes to existing plants is covered in Chapter 16.

Specific expertise in human and organizational factors is now in demand – both by EDF and IRSN – to analyse significant events and search for their organizational or human origin, using methods that have been refined over time. Analysis of these events aims to find not only direct causes, but also root causes, given that:

- technical failures are contingent on human and organizational failures;
- human errors are only symptoms of deeper organizational failures; therefore, excessive focus on the activity or behaviour of operators alone should be avoided.

The rules and practices implemented in event analysis are presented in Chapter 21.

Several events occurred in 1989-1990 during unit outages in reactors belonging to the French nuclear power plant fleet. They were mainly operating errors made while

[188] Oral communication is considered as 'secure' when the speaker is able to send information clearly and completely and then receives confirmation that the information delivered has been properly understood by the recipient.

[189] At the turn of the century, IRSN also analysed how human and organizational factors were taken into account in the design and operation of nuclear facility projects such as the Jules Horowitz research reactor and the Industrial Centre for Geological Disposal (*Centre industriel de stockage géologique*, Cigeo).

using permanent equipment (setting errors on valves used to control configuration of measurement sensors, referred to as 'line-up' errors) and errors due to temporary measures and devices left in place inadvertently after maintenance work. These events led EDF to analyse their causes and to implement corrective measures, particularly for maintenance operations. This subject is discussed in Section 22.2.

In power plants that are in service, analysis of human and organizational factors covers a broader scope of activity, touching on numerous subjects. In addition to operating experience feedback and the organization of control room activities mentioned above, the following subjects have been studied:

– skills management and training for operations personnel,
– organization of maintenance activities and their evolution, including subcontractor management,
– management of emergency response situations.

These areas must obviously be scrutinized continuously by both EDF and safety organizations.

Taking into account human and organizational factors in nuclear power plants in service is covered in Chapter 25.

4.6. Human and organizational factors in French regulations

In 1984, the French Quality Order[190] enacted a certain number of requirements pertaining to quality in the design, construction and operation of basic nuclear installations (including the concepts of 'defined requirements' and 'quality-related activities' for equipment important to safety). Some of the subjects covered in these requirements were related to human and organizational factors such as organization, technical and human resources, competencies (personnel training, qualification, certification), control of quality-related activities, supplier surveillance, document management, processing technical anomalies and incidents, etc.

Until 2012, this order was the regulatory basis that allowed safety authority inspectors, supported by human and organizational factors specialists from IPSN and later IRSN, to carry out inspections in these different areas. These regulatory provisions were reworked and extended by the INB Order of 7 February 2012 discussed in Chapter 2, which prescribes the implementation of an 'integrated management system'[191], sets requirements applicable to activities important for 'protected interests' and requirements for overseeing subcontractors, as well as requirements for

[190] Order of 10 August 1984, discussed in Chapter 2.

[191] "The operator shall define and implement an integrated management system to ensure that requirements pertaining to protected interests [as defined in regulations] are systematically taken into account in any decision concerning the facility."

considering human and organizational factors in the analysis of significant events. Decree 2016-846 of 28 June 2016 introduced additional requirements applicable to subcontracting.

Since 2004, the safety authority, aware of the growing importance of human and organizational factors for safety, has placed greater focus on these factors in its inspection activities and has hired specialists, organized systematic training for inspectors and prepared specific inspection guides for this purpose.

Following the Fukushima Daiichi nuclear power plant accident, which revealed the importance of societal aspects, ASN also decided to open the scope of its discussions on human and organizational factors to various components of society, with the creation in 2012 of a pluralist and interdisciplinary body, the Steering Committee for Human, Social and Organizational Factors (*Comité d'orientation sur les facteurs sociaux, organisationnels et humains*, COFSOH). Within the committee, five working groups deal with subcontracting, legal issues, emergency response management, the relationship between 'regulated' and 'managed' safety, and facility decommissioning activities. The committee's reports are made public[192].

[192] They can be consulted on the ASN website at https://www.asn.fr/L-ASN/Comite-sur-les-facteurs-sociaux-organisationnels-et-humains.

Part 2

Safety by Design

Chapter 5

The Development of Nuclear Power Using Uranium-235 Fission – A Few Notions of Physics Used in Pressurized Water Reactors

5.1. Important milestones in the development of nuclear power using fission of the uranium-235 isotope

Before discussing the safety aspects of pressurized water reactors in the French nuclear power plant fleet, it seemed appropriate to review some of the basic principles that determine how a reactor core operates. This chapter focuses on controlling chain reactions as well as the thermodynamic and thermal-hydraulic aspects related to the release of power, which is particularly important with regard to preserving the first confinement barrier formed by the fuel rod cladding (confinement barriers are described in Chapter 6). For the most part, these basic concepts are discussed here to provide a basis of understanding for the following chapters. Several sources can be consulted by readers seeking more in-depth information on this subject[193].

[193] The following sources may also be cited: Nuclear Reactor Engineering, S. Glasstone & A. Sesonske, Van Nostrand Reinhold Company, 1967, *Traité de neutronique* (Treatise on Neutron Physics), J. Bussac & P. Reuss, Éditions Hermann, *Physique des réacteurs nucléaires* (Nuclear Reactor Physics), R. Barjon (provides some historical information discussed briefly in this chapter), and sources in the *Génie Atomique series*, EDP Sciences, including the article *Physique, fonctionnement et sûreté des REP* (Physics, Operation and Safety of PWRs) by B. Tarride.

Since nuclear reactor design is based on neutron physics studies, this chapter discusses certain aspects of neutron physics, i.e. the study of the pathways taken by neutrons in matter and the conditions required to produce a nuclear chain reaction. Some of the computation tools and methods used in neutron physics will be covered in Chapter 40[194].

The path that led to the first nuclear reactors was marked by important dates, summarized below:

- 1932: evidence supporting the existence of the neutron is obtained by James Chadwick, 40 years after the discovery of radioactivity – and ten years after Rutherford's hypothesis on the existence of a neutral particle predicted to have approximately the same mass as the proton. This year also saw the first nuclear reaction, caused by protons on a lithium target (John Cockcroft and Ernest Walton);
- 1933: Léó Slizárd files for a patent on the chain reaction concept;
- 1934: Enrico Fermi identifies the process underlying the slowing of neutrons (moderation) brought about by collisions with light nuclei (hydrogen, carbon)[195], which increases the probability of nuclear reaction. This discovery contributes to his fame, bringing him the Nobel Prize in Physics in 1938;
- 1938: Otto Hahn and Fritz Strassmann provide evidence of uranium fission by neutron bombardment;
- 1939: at the Collège de France, Frédéric Joliot, Hans von Halban and Lew Kowarski successfully demonstrate by experiment the possibility of a chain reaction, and file a patent application for a reactor (early in 1940, the same team arranges the purchase of the world's entire available stock [180 litres] of heavy water, identified as a moderator, in Norway). Also in 1939, following a letter from Albert Einstein to President Roosevelt, Enrico Fermi obtains grants to acquire one and a half tonnes of graphite as a moderator in order to pursue his work. In the same period, the uranium-235 isotope is identified by Niels Bohr as the fissile element in natural uranium;
- 1942: first measurements of delayed neutrons (defined below) produced by fission of uranium-235, carried out in Chicago by Arthur H. Snell. Also in 1942, after a series of 'exponential experiments' in New York (University of Columbia) then at the University of Chicago, Enrico Fermi achieves 'criticality' (i.e. conditions sustaining the nuclear chain reaction) of the first 'atomic pile' using natural uranium and graphite (Chicago Pile 1, installed under the stands of the Stagg Field stadium on the university campus – see Figure 5.1). Pile 1 is used

[194] Readers may also refer to *La neutronique* (Neutron Physics), CEA/*Éditions Le Moniteur* (monographies written by the Nuclear Energy Directorate).

[195] This work included his well-known experiment performed with paraffin wax (chemical formula C_nH_{2n+2}).

for experiments until 1943, when it is shut down and the decision is taken to dismantle it;

- 1948: for the first time in France, an atomic pile, named ZOÉ, located at Fontenay-aux-Roses, is brought to criticality (see Figure 5.1);
- 1956: criticality reached on the first French nuclear reactor for power generation: the G1 reactor located at Marcoule (an air-cooled natural uranium reactor, using graphite as moderator, prefiguring the future French 'UNGG'[196] series – natural uranium, graphite moderator, gas-cooled reactors [GCRs]);
- 1957: commissioning of the first pressurized water reactor power plant at Shippingport, Pennsylvania, USA.

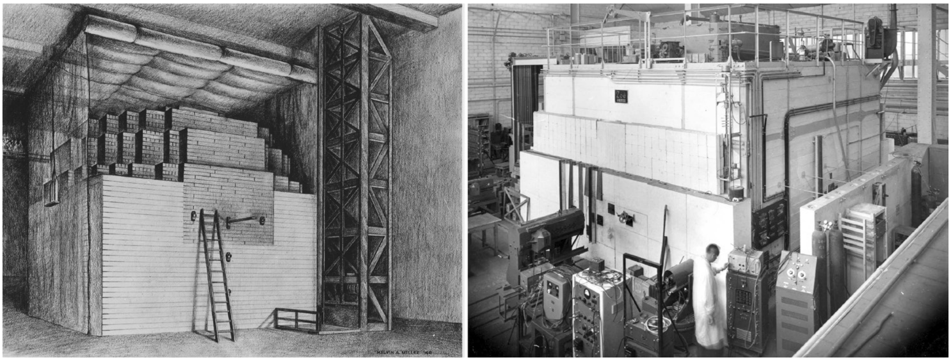


Figure 5.1. Left, Chicago Pile 1 at the University of Chicago. Courtesy of National Archives; right, the ZOÉ pile at Fontenay-aux-Roses. CEA/Documentation Department.

A certain number of concepts are reviewed in the rest of this chapter, in particular nuclear fission, prompt neutrons, delayed neutrons, neutron spectrum, power and reactivity, neutron poisoning and feedback phenomena. One of the important characteristics of nuclear reactors is that when the chain reaction is stopped, they still generate 'residual' heat (including 'decay' heat) over a very long period, another aspect covered in this chapter.

Controlling the chain reaction is part of the nuclear reactor 'process' in both power reactors and experimental reactors, as the objective is to reach the 'critical' state (or 'criticality') for normal operation, i.e. a self-sustaining chain reaction, by 'subcritical approaches' to controlled states of criticality. It will be seen in Chapter 6 that controlling the chain reaction (or 'reactivity', the commonly used term, defined below) is one of the three fundamental safety functions. However, that has not prevented the occurrence of several accidents in experimental reactors, during which control of the chain reaction was lost, not to mention the Chernobyl accident. It should also be recalled that a natural, self-sustaining (without human intervention) nuclear reaction

[196] *Uranium naturel, graphite gaz.*

took place in the Oklo uranium mine operated by Cogema in Gabon. Discovered in 1972, it is the only known case.

In a nuclear reactor, however, criticality must be avoided in all states in which it is not actively sought, for example in shutdown states, when reloading fuel assemblies.

In general, the conditions required to achieve a chain reaction result from an optimum balance between:

- a sufficient quantity of 'fissile' materials ('critical' mass),
- a sufficiently low quantity of neutron absorbing materials,
- favourable geometry, limiting neutron leakage out of the fissile medium,
- if necessary, the presence of a 'moderator' material to reduce the energy of the neutrons produced by fission, in order to increase the probability of generating further fission.

The main fissile materials are uranium-235 and plutonium-239. Other less common isotopes are also fissile, such as uranium-233, plutonium-241, plutonium-238[197], neptunium-237 and californium-251. The only isotopes used in a pressurized water reactor are:

- uranium-235 at a ratio (of enrichment) from 3 to 4.5%, the rest being uranium-238;
- plutonium-239 in fuel assemblies using MOX fuel, with an average plutonium content[198] of 8 to 9% (the use of MOX fuel will be discussed in Section 5.7 below).

When produced, i.e. after fission, neutrons have an average kinetic energy of 2 MeV. In pressurized water reactors, which operate using 'thermal' neutrons (with an average energy of 1/40 eV[199]), water acts as both coolant and moderator, which reduces the fraction of high-energy neutrons and thus increases the probability of fission of uranium-235 nuclei.

In terms of neutron capture, the nuclei of beryllium, zirconium and lead are relatively transparent to neutrons, which is one of the reasons why zirconium alloys are chosen for fuel rod cladding in pressurized water reactors[200]. However, in order to control the chain reaction, neutron-absorbing materials, acting as neutron 'poison', are also needed. Boron, cadmium, gadolinium and hafnium are used most often for this purpose. Other elements commonly encountered also have neutron-absorbing capability, including iron, nickel, chromium, copper, nitrogen, hydrogen, uranium-238 and plutonium-240.

[197] In fast neutrons (see below).

[198] Plutonium isotopes 239 and 241.

[199] Higher energy neutrons are referred to as 'fast' neutrons.

[200] At first Zircaloy-4 (or Zy-4) was used in pressurized water reactors, but this material has been upgraded over time to take into account operating experience (a topic discussed in Section 28.2).

Reflector materials around nuclear reactor cores can limit leakage of neutrons by reflecting them back towards the fissile medium. Water and hydrogenated materials are excellent reflectors, but beryllium, lead and graphite are still more effective. A heavy reflector was developed for the Flamanville 3 EPR, consisting of a 95% steel metal structure, 20 cm thick, with vertical channels for cooling. The reflector also reduces the irradiation fluence[201] received by the reactor vessel material, phenomenon that gradually makes the material less ductile.

It should also be noted that neutron leakage decreases as the ratio of core surface area to core volume becomes smaller[202].

Controlling the reactivity of a reactor involves acting on one or more terms of the neutron balance: those that limit neutron production, those that affect neutron capture and those that favour neutron leakage.

5.2. Fission and important concepts in reactor kinetics

▶ Fission

The fission reaction is shown schematically in Figure 5.2 below.

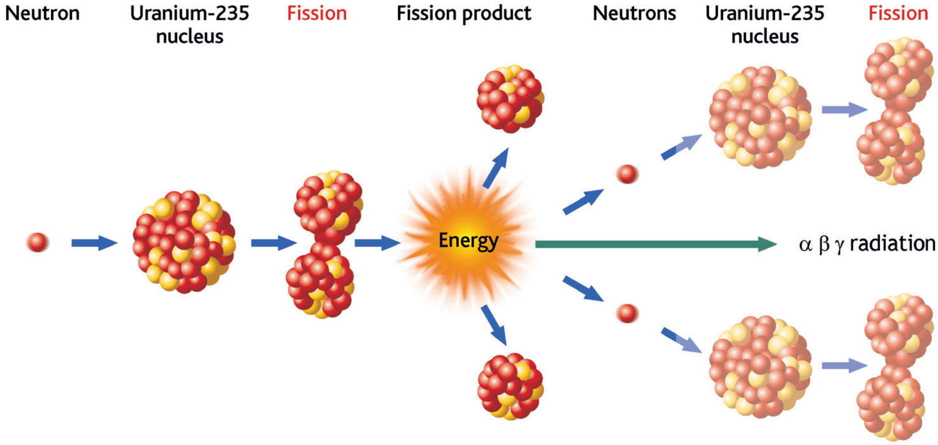


Figure 5.2. Uranium-235 fission reaction. Georges Goué/IRSN.

In a pressurized water reactor, fission of a uranium-235 nucleus generates on average 2.48 ‘secondary’ neutrons (only two are shown in Figure 5.2), capable, in turn, of producing fission in other uranium-235 nuclei. The main fission products are isotopes

[201] Integral over time of the neutron flux received by the vessel material.

[202] More precisely, the surface area of a reactor determines the amount of neutron leakage, while volume determines the quantity of neutrons produced. The ratio of surface area to volume is the lowest for a sphere, which implies that the ratio of leakage to production is also the lowest in a sphere.

of bromine, krypton and zirconium (mass number about 95), and isotopes of iodine, xenon and barium (mass number about 139). Fission products also include isotopes of caesium and ruthenium, which, along with iodine-131, make a major contribution to the radiological consequences in the event of a pressurized water reactor accident.

Fission of a plutonium-239 nucleus generates on average 2.90 secondary neutrons.

The neutron spectrum of uranium-235 fission, i.e. the distribution of the neutrons according to their kinetic energy, is shown in Figure 5.3. Energy peaks at about 1 MeV, and averages 2 MeV (corresponding to a neutron speed of 20,000 km/s).

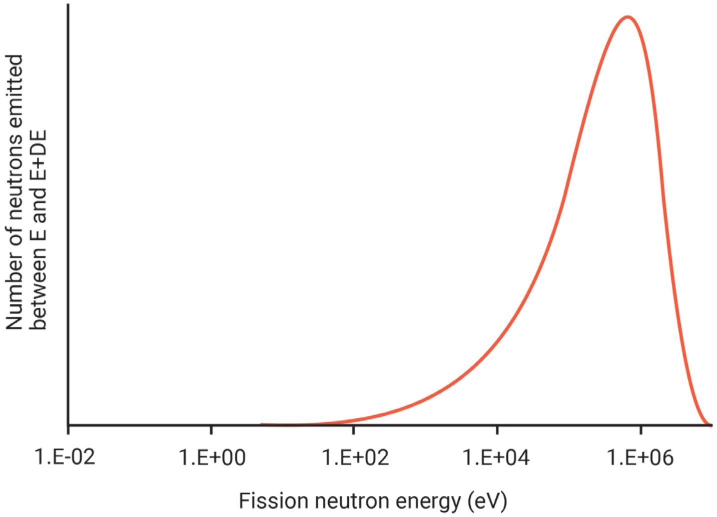


Figure 5.3. Spectrum of neutrons generated by uranium-235 fission (distribution of the number of neutrons that have an energy level between E and E + dE). Georges Goué/IRSN.

As stated above, the water used as moderator reduces the energy of the neutrons, 'displacing' it towards the 'thermal' region, thereby favouring the fission of the uranium-235 nuclei – although there is still a majority of high-energy neutrons in the medium[203].

The amount of energy released by the fission reaction of a uranium-235 nucleus is given by the difference between the energy in the final state and the energy in the initial state, about 200 MeV. Fission of one gram of uranium-235 thus releases about 8.2×10^{10} joules of energy, equivalent to approximately one megawatt-day (MWd). Fission of all the uranium-235 nuclei in one tonne of natural uranium containing 0.7% uranium-235 generates 10,000 times more energy than one tonne of oil equivalent.

[203] The boundary between the thermal-neutron region and the fast-neutron region is defined at the energy value of 0.625 eV. In pressurized water reactors, the ratio between the flux of neutrons with energy greater than 0.625 eV and the flux of neutrons with energy less than that value is between 5 and 6.

▶ A few important concepts in reactor kinetics

The term ‘reactor kinetics’ refers to the behaviour of a nuclear reactor over time (neutron population changes) and the parameters that determine this behaviour. This section discusses notions important to understanding reactor kinetics.

For convenient expression of the conditions for sustaining the chain reaction, it is customary to consider the effective multiplication factor, *keff*, given by the ratio:

$$keff = \frac{\textit{number of neutrons in one generation that produces a fission}}{\textit{number of neutrons in the preceding generation that produces a fission}}$$

Reactivity, ρ, is given by the following ratio:

$$\rho = \frac{keff - 1}{keff}$$

Reactivity thus represents the fraction of neutrons missing or in excess for sustaining the chain reaction. It is expressed in pcm (per cent mille: 10^{-5}).

The effect on power is summarized in the table below:

keff	< 1	1	> 1
ρ	< 0	0	> 0
Reactor state	subcritical	critical	supercritical
Power	decreasing	stable	increasing

The time profile of the neutron population is given by the function below (excluding delayed neutrons [see below] and without an additional neutron source):

$$\frac{dn}{dt} = n\,\frac{(keff - 1)}{\ell}$$

where ℓ is the average lifetime of the neutrons *n*.

The reactor period, *T*, time required for the neutron population to be multiplied or divided by the factor e (2.718), is therefore given by:

$$T = \frac{\ell}{keff - 1}$$

In practice, at this stage these are highly simplified formulations, because of a fundamental aspect of how a reactor operates: a small fraction of the neutron population is emitted with a delay with respect to the neutrons generated directly by fission, and no reactor would be controllable without these **delayed neutrons**. They are therefore distinguished from the neutrons generated directly by fission, referred to as **prompt neutrons**. The fraction of delayed neutrons is referred to as 'β-effective', or *βeff*. Most of the neutrons involved in the chain reaction are released directly, practically at the time of fission (with a time delay of about 10^{-14} s). Their lifetime is short: 25 μs for water reactors. In contrast, the relatively few delayed neutrons are released by radioactive decay of certain fission products, with a delay[204]. Their overall contribution depends on the fissile nuclei: about 1450 pcm for uranium-238, 650 pcm for uranium-235 and 210 pcm for plutonium-239[205]. The *βeff* fraction depends on the proportions of these elements. For French pressurized water reactors loaded with uranium, *βeff* varies between 500 and 700 pcm.

When reactivity is greater than *βeff*, the time separating two generations of neutrons becomes very short. The reactor then becomes critical or supercritical with prompt neutrons only; power variations can then be extremely rapid.

Another variable used is **neutron flux**, i.e. the quantity of neutrons passing through a surface per unit of time, represented by the symbol ϕ. In a pressurized water reactor, with a population of 50 to 150 million neutrons per cubic centimetre, neutron flux is 1 to 3 × 10^{13} neutrons × cm^{-2} × s^{-1}, i.e. 100 times lower than the fluxes obtained in reactors with a higher energy spectrum, such as the high-flux reactor located in Grenoble (10^{15} neutrons × cm^{-2} × s^{-1}), or the PHENIX fast-neutron reactor (about 7 × 10^{15} neutrons × cm^{-2} × s^{-1} at the centre of the core[206]) which was shut down definitively in 2009.

▶ Neutron feedback phenomena

In addition to delayed neutrons in the neutron population, two other effects contribute to controlling pressurized water reactors: the Doppler effect and the moderator effect. These two effects constitute what is referred to as 'neutron feedback'.

The Doppler effect results from the power decrease (reduction in the number of fissions) that occurs when the fuel temperature rises. In a pressurized water reactor, the Doppler effect is about -3 pcm/°C. It is related to the increase in neutron capture[207] by uranium-238 when the fuel temperature increases (see Figure 5.4). Physically, this is due to an increase in the probability of neutron capture by uranium-238 as the temperature of the uranium-238 nucleus rises – a process known in scientific literature as 'Doppler broadening of resonances'. It occurs practically instantaneously and is intrinsically stabilizing. It plays a very important role in the control of power increase

[204] The delayed neutron emitters decay with half-lives between a few tenths and a few tens of seconds.

[205] These values are given for the case of fission within a spectrum of fast neutrons, but differ only slightly for a spectrum of thermal neutrons. Some countries use *βeff* as a unit of reactivity, usually referred to as dollar units, with the symbol $; this unit and symbol are generally adopted for fast-neutron reactors.

[206] *Phénix, le retour d'expérience* (PHENIX Operating Experience Feedback), J. Guidez, published by CEA.

[207] Refer to the sources cited previously in this chapter for details on the concepts of fission cross section, capture cross section and others.

transients, independently of any automatic or manual actions that might be taken. It should be noted that when reactor power is 'ramping up', the reactivity to be released (by reducing the boron concentration in the reactor coolant and gradually withdrawing the control assemblies) must oppose the negative reactivity corresponding to the integral of the Doppler effect from the shutdown state to the targeted operating temperature.

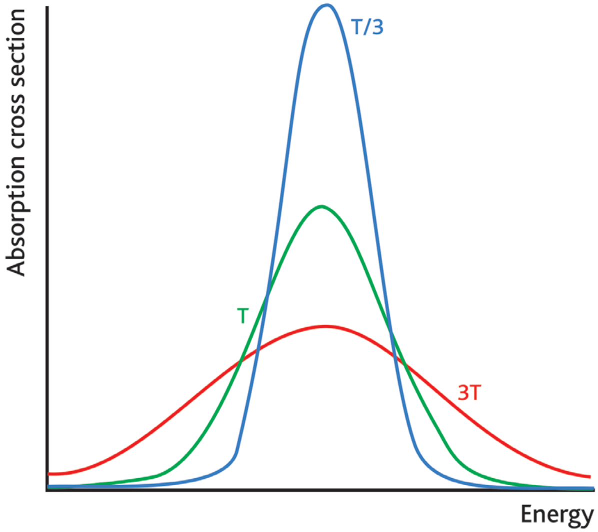


Figure 5.4. Schematic representation showing the widening of the curve of the absorption cross-sections of uranium-238 as a function of the energy of the impacting particle at three temperatures of uranium-238: T, T/3 and 3T. IRSN.

The second beneficial effect in a pressurized water reactor comes from the moderator, i.e. the water in the primary system referred to as the 'reactor coolant'. In a pressurized water reactor, the water slows the neutrons ('thermalization'), thus favouring the fission of uranium-235 nuclei. It is clear that if the water expands (for example, if its temperature rises or in the event of depressurization) or even disappears (through boiling or draining), the chain reaction gradually stops. This is an important phenomenon for the control of certain transients, which depends, however, on the kinetics of temperature variation or the proportion of water. Between the beginning[208] and end of a reactor core operating cycle (and assuming that xenon is 'at equilibrium' – see below), the effect of the moderator (also referred to as the moderator temperature coefficient) changes from about -10 pcm/°C to -60 pcm/°C. This change in the moderator effect as the cycle progresses is due to the effect of boron, an absorbing element added to the water in the reactor coolant system. The boron concentration is reduced as core fuel burnup progresses (refer to Section 5.6 below).

[208] Reactor core operating period between two refuelling (and maintenance) outages.

The ratio of the concentration of moderating atoms per unit volume to the concentration of fissile atoms per unit volume, known as the moderation ratio, is one of the core design options. In the case of pressurized water reactors, the core is designed to function with an 'under-moderated' fuel rod lattice obtained by carefully calculating the space between rods, so that any rise in the water temperature, especially at boiling point, lowers the effective neutron multiplication factor.

Figure 5.5 shows the profile of the multiplication factor *keff* as a function of the moderation ratio and the selected design option:

- the more tightly spaced the fuel rod lattice, the less the amount of moderator present is capable of slowing the neutrons (low moderation ratio, left-hand part of the curve): the multiplication factor decreases;
- the more widely spaced the fuel rod lattice, the less the probability that a neutron emitted in the fuel and thermalized in the moderator will collide with another fissile atom (high moderation ratio, right-hand part of the curve): the multiplication factor decreases;
- there is an intermediate situation in which the moderation ratio leads to the peak multiplication factor (optimum moderation).

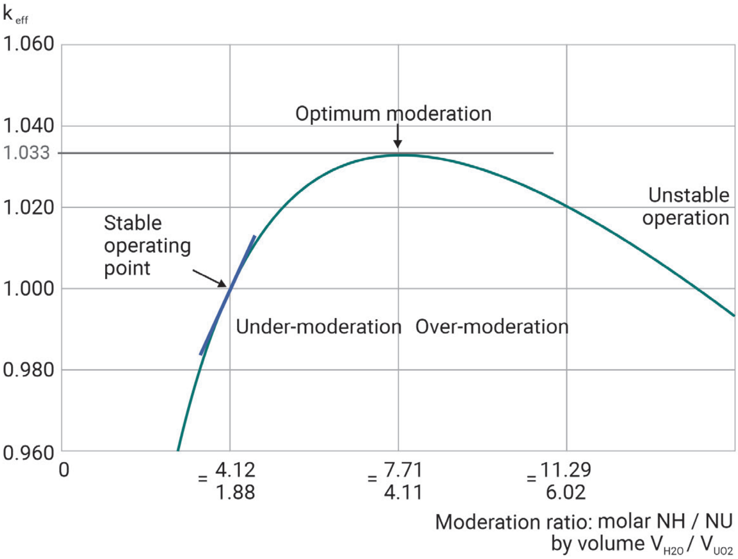


Figure 5.5. Variation of *keff* as a function of the moderation ratio. Source: Internovice CC BY-SA 3.0.

The Doppler effect and the moderator effect thus both act in the same direction with regard to temperature variations:

- an increase in coolant temperature introduces negative reactivity;
- conversely, cooling introduces reactivity (for example, when a steam generator relief valve opens).

▶ An aspect of neutron physics in pressurized water reactor cores: the xenon effect

An important phenomenon to be considered in the cores of thermal neutron reactors such as pressurized water reactors is related to xenon. Fissions produce iodine-135, which decays in a few hours to xenon-135, which in turn also decays in a few hours, absorbing neutrons generated by fissions[209]. When power is reduced or the reactor is shut down, there are no longer enough neutrons to ensure xenon-135 decay, so it accumulates, 'poisoning' the reactor. A 'xenon peak' is reached approximately ten hours after reactor shutdown (see Figure 5.6). If the reserve of reactivity in the core is insufficient, the reactor cannot be restarted at that time. In the longer term, the gradual depletion of xenon-135 contributes excess reactivity with respect to the initial state of the reactor at power, which must be compensated by increasing the boron concentration in the reactor coolant. In stable normal operation at full power, the production and depletion of xenon-135 reaches equilibrium after about 50 h (neutron absorption by xenon representing approximately 3000 pcm).

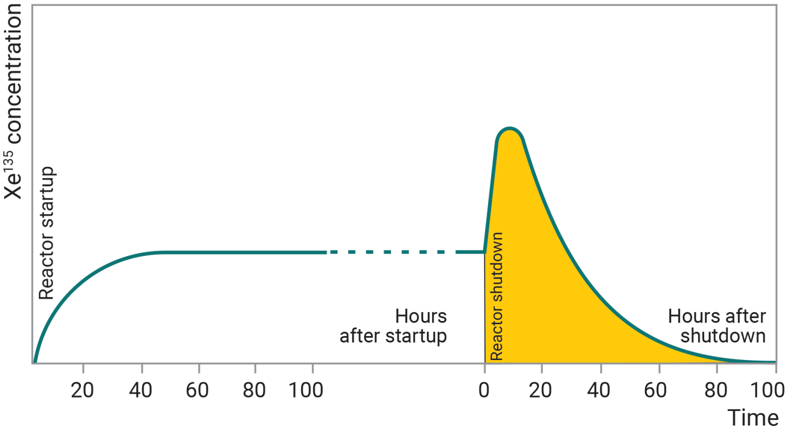


Figure 5.6. Profile of the xenon-135 concentration during pressurized water reactor operation. IRSN.

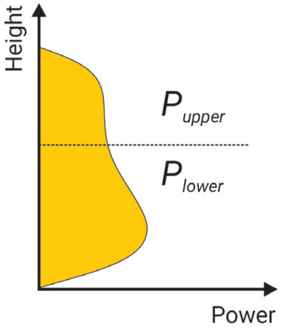
The negative reactivity related to the xenon concentration may be the source of radial or axial power instability or oscillations in the core. A local power increase can lower the xenon concentration by increasing neutron absorption by xenon, which in turn boosts the power increase until poisoning is in equilibrium with the new power distribution. The xenon-related instability or oscillations last for about 24 h, but can be controlled using the control assemblies, through continuous monitoring of the 'axial offset' described below.

[209] Neutron absorption by xenon is highest in the thermal-neutron region.

▶ Parameters describing neutron flux heterogeneity within the core

Axial distortion of neutron flux in the core is represented by the axial offset (AO), given by the ratio below (where *P* is nuclear power):

$$AO = \frac{P_{upper} - P_{lower}}{(P_{upper} + P_{lower})\ nominal}$$



Two other variables representative of the power distribution in a reactor core are used, for example in the algorithms of the reactor protection system (refer to Section 5.6):

- **hot-spot factor F_Q**:

$$F_Q = Max\,[P(x,y,z)]_{x,y,z}$$

- **radial hot-channel factor $F_{\Delta H}$**:

$$F_{\Delta H} = Max_{x,y} \int_z P(x,y,z)$$

Another noteworthy concept concerning power distribution in the core is '**power tilt**'. The reactor core is built so that the fuel is loaded symmetrically, with the aim of obtaining a symmetrical power distribution that is as uniform as possible. For reasons not fully understood (probably related to a possible curvature of some fuel assemblies in the core, resulting in variations of the width of the water gap between fuel assemblies, and consequently the moderation ratio), the power distribution may not be symmetrical, resulting in a difference between the average power of one of the core quadrants and that of the other three quadrants. Power tilt was observed in the 900 MWe reactors, but higher levels were observed in 1984 during startup tests on Unit 1 at the Paluel nuclear power plant, the first-off unit of the 1300 MWe series reactors, with values reaching 5 to 10%. In safety studies, the hot-spot factors defined above are increased by a coefficient to take into account any differences due to possible power tilt. The associated penalties are validated by checking power tilt limits during the physics tests conducted when restarting a reactor after refuelling.

5.3. Removing power from the core during operation

As stated above, the fission of one gram of uranium-235 releases about 8.2×10^{10} joules of energy, i.e. about 1 MWd.

Most of this energy (82%[210]) is released in the form of kinetic energy from the excited and radioactive fission products, which in turn release energy in forms such as beta and gamma radiation, also carrying away a small part of the reaction energy. Furthermore, as the fission products have very short paths in the material, their kinetic energy is dissipated locally in the fuel as heat.

In a pressurized water reactor, the heat released by the fuel is dissipated by heat transfer through the zirconium alloy cladding and by circulation of coolant (the reactor coolant system water) around the fuel rods.

Typical operating parameter values are given in the table below (values for the 1450 MWe N4 series reactors):

Thermal power removed from the core (N4 series)	4250 MW
Reactor coolant system pressure	155 bars
Reactor vessel inlet water temperature	292°C
Reactor vessel outlet water temperature	329°C
Water heating in the reactor	37°C
Average water temperature in the core	310°C
Reactor coolant system flow rate at reactor vessel inlet	95,580 m^3/h

These operating parameters are associated with:

- a maximum fuel temperature at the centre of the pellets of about 1000°C, compared with the melting point of uranium oxide UO_2, which is 2810°C for fresh fuel and decreases[211] by 7.6°C every 10,000 MWd/t (the melting point of UO_2-PuO_2 mixed oxide is 2757°C, which decreases by 4°C every 10,000 MWd/t);
- a maximum cladding temperature of about 350°C, compared with the melting point of zirconium, 1855°C[212].

At a pressure of 155 bars, water boils at approximately 340°C, about 11°C above the core outlet water temperature.

5.4. Decay heat

Energy release in fuel involved in a chain reaction does not stop when the reaction is stopped (Table 5.1). Fission products alone must release a certain amount of energy in the form of radioactivity before reaching a stable state. Each radioactive isotope in the fission products has its own radioactive half-life; this half-life may be very short

[210] According to M. F. James, Energy Released in Fission, Journal of Nuclear Energy, Vol. 23, 517-536 (1969). The kinetic energy of secondary neutrons accounts for only 2.4% of the total fission energy.

[211] Due to the changing chemical composition of the fuel.

[212] But the integrity of the cladding may be lost well below this melting point depending on the thermal-mechanical loads to which it is subjected.

(less than a second), average (months or years) or very long (hundreds or thousands of years). Although decreasing, the power generated is greater than a thousandth of the nominal power for a long time, requiring continuous cooling at a certain level.

Table 5.1. Decay heat of a reactor core over time – case of a 3000 MWth reactor, i.e. about 1000 MWe, at end of cycle, loaded with uranium oxide, for maximum burnup in the core (averaged over each assembly) of 33 GWd/tU.

Time since shutdown	Initial proportion of thermal power	Thermal power generated (MW)
30 seconds	7 to 8%	210 to 250 MW
1 minute	5%	150
1 hour	1.5%	45
1 day	0.5%	15
1 week	0.3%	9
1 month	0.15%	4.5
1 year	0.03%	1
10 years	0.003%	0.1
100 years	0.001%	0.03
1000 years	0.0002%	0.006

5.5. Main features of pressurized water reactor cores

The main core characteristics in the different series of French pressurized water reactors are given in Table 5.2, and a fuel assembly is shown in Figure 5.7.

Table 5.2. Main core characteristics in the different series of French pressurized water reactors.

Reactor type	900 MWe	1300 MWe	N4	EPR
Number of fuel assemblies	157	193	205	241
Number of fuel rods per assembly	264 (17 x 17 lattice with 24 guide tubes and one instrumentation tube)			265 (the instrumentation tube is replaced by a fuel rod)
Rod (cladding) outside diameter/ cladding thickness (zirconium alloys)	9.50 mm/0.57 mm			
Fuel pellet stacking height ('active' part of the core)	3.66 m (UO_2) or 3.59 m (MOX) (12 feet)	4.27 m (14 feet)		4.20 m (~14 feet)
Fuel assembly length	4.06 m	4.80 m		4.80 m
Fuel assembly width	21.4 cm			
Number of guide tubes in control assemblies	24			

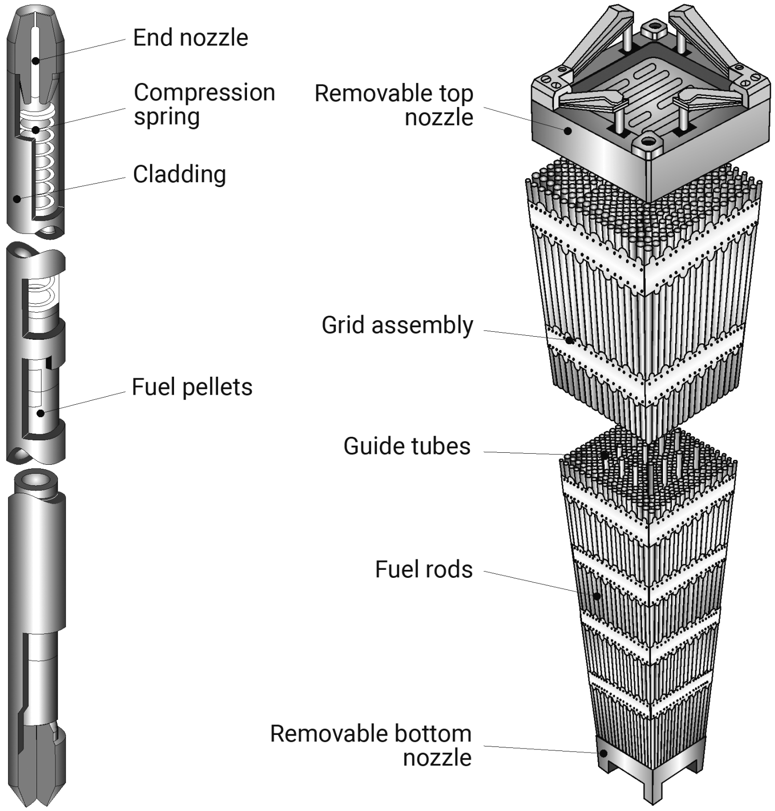


Figure 5.7. General view of a fuel rod and a fuel assembly. Georges Goué/Médiathèque IRSN.

The various ways to use fuel assemblies in reactor cores and their associated characteristics (such as the burnup rate when they are unloaded), representing the key elements of 'fuel management', are discussed in Chapter 28.

5.6. Control and monitoring of pressurized water reactor cores

As seen above, controlling the power generated in the reactor core assumes that core reactivity is controlled by two different but complementary means: the boron concentration in the reactor coolant and movable neutron absorbers inserted into the core. It was also explained that the choice of an under-moderated lattice of fuel assemblies contributes to core stability with regard to temperature increases (the volume of water between the fuel rods is slightly below the volume that would ensure optimum neutron slowing); the Doppler effect is the other stabilizing phenomenon.

Two types of movable neutron absorbers (hereafter referred to as 'rod cluster control assemblies', or RCCA) are used:

- control RCCAs: when the reactor is in operation, they are inserted into the 'active' part of the core (fissile zone) to regulate the reactor coolant temperature and power in function of the external demand for electricity; some control assemblies can be fully inserted into the core in reactor shutdown states;
- shutdown RCCAs: when the reactor is in operation, these assemblies are positioned above the active part of the core; they are dropped by gravity, along with the control RCCAs, to shut down the reactor in the event of an anomaly. In shutdown states, the shutdown RCCAs are inserted in the core, except for some that remain withdrawn to provide an available source of negative reactivity, for example in the event of inadvertent boron dilution[213].

The number of RCCAs in the different reactors is given in Table 5.3.

Table 5.3. Number of RCCAs in different reactors.

Reactor type	900 MWe	1300 MWe	N4	EPR
Number of RCCAs (both control and shutdown RCCAs)	Between 48 and 57, depending on the fuel management scheme	65	73	89

The quantity of fissile material inserted in the core during a normal refuelling outage is calculated to allow the reactor to operate for at least one year. Available reactivity is controlled by control RCCAs and by boron dissolved in the reactor coolant. The insertion of strong neutron-absorbing RCCAs, however, disturbs the neutron flux significantly and consequently impacts the power generated locally, inducing mechanical stress on the cladding. Strong 'black' RCCAs are used for shutdown or for certain power and temperature control configurations. Less-absorbing 'grey' RCCAs were introduced for the series of reactors designed after the first plant series referred as CP0, as they limit the neutron flux disturbance caused by their insertion. RCCA compositions are given in Table 5.4.

[213] The EPR differs from this process in that all the RCCAs are inserted in reactor shutdown states. This is made possible by specific systems that are used on this reactor to prevent the risk of uncontrolled criticality in the event that reactivity is inserted in any given shutdown state. These systems include a mechanism to automatically cut the electrical power supply to the RCCA drive mechanisms in these states, eliminating the risk of uncontrolled withdrawal, and automatic protection against uncontrolled boron dilution incidents in the reactor coolant system (see Chapter 35).

Table 5.4. Composition of RCCAs[214].

Reactor types → **Types of RCCAs** ↓	**900 MWe**	**1300 MWe, N4 and EPR**
Assemblies with 'black' absorber rods	24 AIC rods (80% silver, 15% indium, 5% cadmium)	24 AIC/B4C (boron carbide) rods
Assemblies with 'grey' absorber rods	8 AIC rods and 16 stainless steel rods *(no grey rods in reactors from the first plant series, referred to as CP0)*	8 AIC rods and 16 stainless steel rods

For reactor control and reactivity management in shutdown states, the drive mechanisms for both control and shutdown RCCAs are grouped into control banks and shutdown banks, respectively. The design of the 'RCCA scheme' depends on the 'control mode' adopted and is the result of several compromises made to favour reactor manoeuvrability while maintaining the necessary safety margins, related in particular to power distribution disturbances, reactor trip performance, and postulated reactivity insertion incidents or accidents due to RCCA withdrawal (see Chapter 35). For example, the insertion depth of the RCCA banks in the core, depending on the level of reactor power, must be sufficient to produce the power variations required to meet demand from the power grid, while remaining limited, so that dropping all the RCCAs ensures rapid reactor shutdown with an adequate shutdown margin (for example, -1800 pcm for 1300 MW reactors using the GEMMES fuel management scheme) and uncontrolled withdrawal of one or more RCCA banks or rapid ejection of the most effective RCCA[215] out of the core have no unacceptable consequences.

Using boron dissolved in water as boric acid H_3BO_3 does not have the same drawbacks, since its distribution is uniform. Its effectiveness is about -10 pcm per ppm (parts per million)[216]. However, its concentration cannot be changed rapidly, and there is a restriction important to safety concerning the maximum boron concentration. Heating the moderator containing neutron poison must be avoided, as this would reduce the density of the poison, causing an increase in core reactivity and a potentially uncontrolled power rise. The moderator temperature coefficient would then be positive, which is forbidden in PWRs.

RCCAs regulate the power and shut the reactor down in an emergency ('reactor trip' – see below). The boron compensates core fissile material burnup and the various effects on reactivity, related in particular to fuel and moderator temperature variations or xenon-135 accumulation. A cold core requires more boron than when operating at

[214] Hafnium is also used as a neutron absorber in control assemblies located along the core periphery to reduce vessel irradiation (see Chapter 27).

[215] It will be seen in chapters 8 and 35 that these are respectively an incident and an accident taken into account in pressurized water reactor design, classified respectively as Category 2 and Category 4 events in the operating conditions.

[216] This proportion is expressed in natural boron. The concentration of boron-10, which is the neutron absorber, is obtained by considering that natural boron contains about 20% of boron-10.

power, as the RCCAs are no longer capable of ensuring core subcriticality on their own in these conditions.

The reactivity that must be controlled by the boron depends on the power generated, the core temperature in operation, hot or shut down, and the fuel assembly burnup rate. When cold, after refuelling, with all RCCAs inserted, the boron concentration needed to maintain core subcriticality is approximately 1000 ppm (parts per million). This is sufficient to control the 12,000 pcm of available reactivity. With certain RCCA banks withdrawn from the reactor core according to the RCCA configurations defined in the various shutdown states, 1450 ppm of boron is required to control the 15,000 pcm of available reactivity. In hot shutdown, with the reactor coolant at 286°C and all shutdown RCCAs withdrawn, about 900 ppm of boron is needed to control the 7000 pcm of available reactivity, the effectiveness of the boron decreasing with the temperature due to the decrease in coolant density (see Figure 5.8).

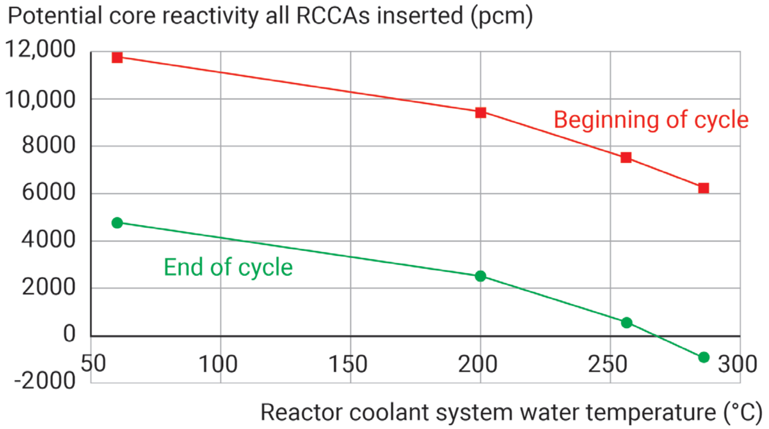


Figure 5.8. Potential reactivity of the core without boron. IRSN.

The reactor operational limits and conditions (refer to Section 20.2) initially required a margin to criticality ranging from 5000 pcm (cold shutdown for core refuelling – vessel open) to 1000 pcm (cold or hot shutdown at beginning of cycle [BOC]), leading to a requirement for boron concentrations between 2000 and 1000 ppm at BOC. However, studies on the risks of a criticality accident by transfer of unborated water into the core, conducted following the Chernobyl power plant accident (see Chapter 35), led Électricité de France (EDF) to subsequently set 2000 pcm as the minimum margin to criticality for the normal shutdown states of the reactor, hot or cold[217]. This gives the operator sufficient time to respond to both slow homogeneous

[217] The boron concentration depends on the stage of the cycle and the temperature of the reactor coolant. For example, at beginning of cycle, with the GEMMES fuel management scheme (see Chapter 28), the boron concentration required varies between approximately 1700 and 2000 ppm when cold and from approximately 1250 to 1700 ppm when hot. At end of cycle, the required boron concentrations are of the order of a few ppm when hot and 960 ppm on average when cold.

dilution of the coolant and heterogeneous dilution. Moreover, for the most recent fuel management schemes implemented by EDF in its reactors, the minimum margin to criticality has been increased beyond 2000 pcm to prevent the risk of a return to power in these normal shutdown states in the event of uncontrolled insertion of reactivity due to RCCA withdrawal or uncontrolled cooling of the reactor coolant (see Chapter 35).

Lastly, the minimum boron concentration required in the shutdown states for core refuelling or for maintenance is now defined so as to ensure a margin to criticality slightly greater than 2000 pcm without any RCCAs in the core (postulating a bounding-case accident situation of withdrawal of all the RCCAs when lifting the vessel cover[218]).

Moreover, the extension of the French nuclear power plant reactor core irradiation cycle (from 12 months to 18 months) has led to an increase in the uranium-235 enrichment of the fuel. Controlling the surplus of reactivity at beginning of cycle therefore required the use of another neutron absorber, gadolinium, to limit the boron concentration in order to ensure a negative moderator temperature coefficient. Gadolinium is consumed as it is irradiated, whence the term 'consumable poison'. It is used in the solid oxide form Gd_2O_3 in fuel pellets.

Many plant design and operating constraints and the design of protection systems and engineered safety systems are determined by the above considerations.

Physics studies and thermal-hydraulic studies must, of course, cover all types of loading, all burnup rates and all reactor states ranging from nominal power to cold shutdown. Any change in the fuel characteristics, such as the introduction of a significant proportion of plutonium oxide mixed with uranium oxide, requires analysis of the consequences in terms of safety.

▶ Parameters monitored in a pressurized water reactor

The general purpose of core protection is to mitigate an abnormal situation so as to meet a number of criteria intended to avoid damaging the confinement barriers, the first of which is the fuel cladding. Although damage may nevertheless occur, it must remain limited to an acceptable level and not affect the ability to cool the core in order to remove any residual heat (this topic is discussed further in Section 8.4.7). In practice, the protection system actuates two types of system:

– the reactor shutdown system, which releases and drops the control and shutdown RCCAs, actuated either automatically or manually by an operator;

– the engineered safety systems (described in Section 6.4.1), which are actuated either automatically or manually by an operator. They include the safety injection system for injecting water into the reactor coolant system, the steam generator emergency feedwater system, the containment heat removal system spraying water inside the containment (reactor building), and the containment isolation system.

[218] This is the most restrictive criterion, but the margin to criticality of 5000 pcm given above nevertheless remains applicable.

This chapter focuses mainly on the part of the protection system that triggers 'reactor trip'[219] (RT) in a few seconds by dropping all the RCCAs into the core, and initiates turbine trip by closing the turbine steam inlet valves.

The RT trigger command (or RT signal) can be given through various protection channels, each channel comprising instruments measuring one or more variables characterizing the state of the reactor, a data processing system, and a system that compares the resulting information with a preset value. If thresholds are exceeded, RT is initiated by deactivating the RCCA drive mechanism electromagnets. The measurements used are redundant and processed according to 'voting logic' (such as '2 out of 4') that transmits the RT signal.

It should be emphasized that the architecture and characteristics of the protection system – in particular the reactor trip signals – are the result of a complex iterative process involving design options, operating transient studies and safety requirements, which cannot be explained in a few lines. As an illustration, although protection of the confinement barriers is the general objective, other requirements come into play, for example avoiding operation of the pressurizer safety relief valves in frequent transients[220], avoiding water release through the pressurizer letdown valves and safety relief valves, or ensuring reactor manoeuvrability.

The variables used to characterize the reactor state are given in Figure 5.9 below.

The basic variables that are measured and the associated measuring instruments are:

- **Neutron flux** (ϕ): measured using a system of detectors located outside the vessel (in detector holders that can be brought as close as 30 cm from the vessel) for each quadrant of the core. In the case of the EPR, the detectors are located in guide tubes penetrating the concrete biological shield around the vessel. The system comprises 'source range' detectors (SRD), 'intermediate range' detectors (IRD) and 'power range' detectors (PRD)[221], which form the ex-core instrumentation system.

  For the 900 MWe, 1300 MWe and 1450 MWe reactors, complementary to the ex-core system, there is an in-core system (ICS) that produces neutron flux maps using periodic measurements taken by movable internal detectors (fission microchambers) deployed through several dozen vessel lower-head penetrations. These in-core measurements are not directly involved in the protection system; they are used to check that the cores comply with the predefined loading patterns, to ensure that any power tilt is acceptable and to establish neutron flux form factors provided as input to the protection system algorithms (see below).

[219] In French *arrêt automatique du réacteur*. The terms '(reactor) scram' and 'emergency shutdown' are also used frequently.

[220] Transients classified as Category 2 of the operating conditions (see Chapter 8).

[221] These different detectors have overlapping measurement ranges that depend on the reactor series; for example, for the EPR, SRDs cover the range 2×10^{-9} to 2×10^{-3}% NP (nominal power), IRDs cover the range 5×10^{-6} to 60% NP, and PRDs cover the range 0.5 to 200% NP.

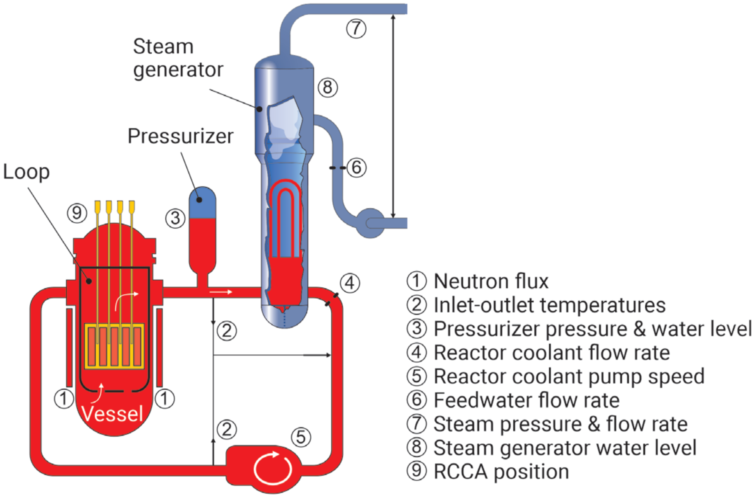

Steam generator
Pressurizer
Loop
Vessel
①
②
③
④
⑤
⑥
⑦
⑧
⑨
① Neutron flux
② Inlet-outlet temperatures
③ Pressurizer pressure & water level
④ Reactor coolant flow rate
⑤ Reactor coolant pump speed
⑥ Feedwater flow rate
⑦ Steam pressure & flow rate
⑧ Steam generator water level
⑨ RCCA position

Figure 5.9. Parameters monitored in a pressurized water reactor. Georges Goué/IRSN.

The EPR[222] has a different in-core system (derived from that of the German KONVOI reactor design) and comprises the following (see Figure 5.10):

- fixed, cobalt-based self-powered neutron detectors (SPNDs) that emit a signal proportional to the neutron flux, installed in 'strings' of six axially-spaced SPNDs, inserted in 12 fuel assemblies (through one of the guide tubes). The SPNDs supply input data to several monitoring and limitation channels[223] and the core protection system;
- an aeroball measurement system (AMS) featuring stacks of movable balls doped with vanadium-51, transported pneumatically to the 'active' zone of the core, in 40 fuel assemblies; the balls are then transferred to a measuring table outside the core for activation analysis.

The AMS (like the fission microchambers of the 900 MWe, 1300 MWe and 1450 MWe reactors) is used periodically to create the neutron flux maps required to check core conformity and to calibrate SPNDs and ex-core systems.

[222] For further details, readers may refer to Article BN3453 V1 in *Techniques de l'ingénieur*, entitled *Instrumentation neutronique du réacteur EPR – Excore – SPND – AMS* (EPR Neutron Instrumentation – Excore – SPND – AMS), by Maxime Pfeiffer, published on 10 July 2014.

[223] For the EPR, this is the Reactor Core Limitation System (RCLS), designed to avoid actuation of the protection functions by initiating action on the control RCCAs sufficiently early to maintain the reactor parameters below the protection function actuation thresholds.

The EPR instrumentation, with detectors inserted through the top of the core, makes it possible to eliminate the vessel lower-head penetrations, thereby improving safety[224], especially in the event of core-melt accidents.

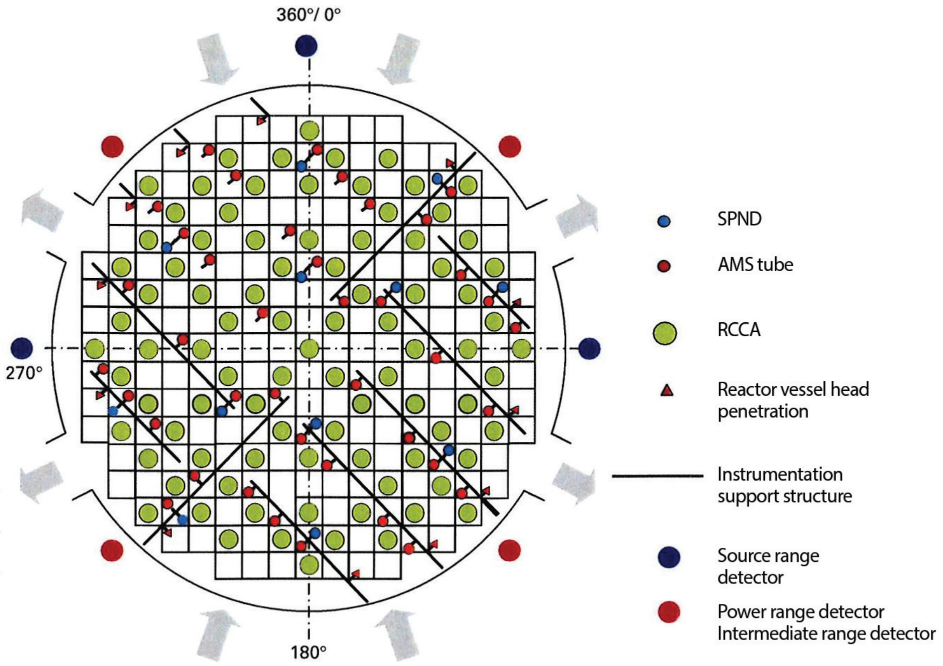

360°/ 0°
270°
180°
SPND
AMS tube
RCCA
Reactor vessel head penetration
Instrumentation support structure
Source range detector
Power range detector
Intermediate range detector

Figure 5.10. Neutron flux instrumentation of the EPR core (showing three of the four source range detectors (SRDs). Source: see Footnote 222.

- **Temperature of the reactor coolant** (i.e. the reactor coolant system water): measured by probes located either in the reactor coolant system loop bypass lines, or measured directly by sampling from the main system pipes.
- **Pressure in the reactor coolant system and the secondary system**: measured by sensors in the pressurizer and in the steam lines.
- **Water flow rates in the reactor coolant system and the secondary system**: measured by differential pressure sensors located in the reactor coolant system loops (at the outlets in the steam generator) and in the steam lines, in addition to reactor coolant pump rotation speed measurements.
- **Water levels** in the reactor coolant system components (pressurizer, steam generators, reactor vessel).

[224] This instrumentation is capable of producing neutron flux maps at power levels of 10% NP and above.

All the variables mentioned above are also used to generate 'permissive' signals (i.e. enabling signals) and interlocks (to block control RCCAs), in addition to control room alarms and reactor trip. These permissive signals adjust the protection system logic to the state of the reactor unit.

Other more or less complex variables are generated from the above variables by various algorithms and contribute in particular to the protection of the first confinement barrier:

- **temporal variation of the neutron flux (*dϕ/dt*)**: derived from the neutron flux measurements made by the ex-core detectors;
- **thermal power (*Pth*)**: derived from the reactor coolant temperature and flow rate measurements, it is calibrated by a periodic power measurement obtained by a secondary-side thermal balance;
- **maximum linear power density (LPD) in the core**: monitoring this variable contributes to protection against the risks of core melting and pellet-cladding interaction (PCI). Determination of this variable and the next (DNBR), requires 'remaking' the core flux map based on signals sent from the in-core system of the EPR or the ex-core system of the 1300 MWe and 1450 MWe reactors (the case of 900 MWe reactors is discussed below);
- **minimum departure from nucleate boiling ratio (DNBR) in the core**: monitoring this variable contributes to protecting the core from the risk of overheating the cladding in the event of departure from nucleate boiling. The DNBR is defined by the following ratio:

$$DNBR = \frac{\phi c}{\phi l}$$

- where ϕc is the critical heat flux, i.e. the heat flux threshold at which departure from nucleate boiling occurs, and ϕl is local heat flux;
- **axial offset (AO)** defined in Section 5.2: monitored on-line during reactor control. The operational limits and conditions impose axial offset limitations to ensure compliance with the assumptions made in the accident studies regarding the axial power distribution.

On-line determination of LPD and DNBR in the protection system was introduced in the mid-1980s on 1300 MWe reactors, with installation of the integrated digital protection system. This type of on-line monitoring of these variables is now implemented on all 1300 MWe and 1450 MWe reactors, and on the EPR. It was not introduced on the protection system of 900 MWe reactors, where protection against the risks of fuel melting and departure from nucleate boiling are based on measuring the reactor coolant system water temperature at the vessel inlet and outlet ('ΔT' channels) and on the other variables above (ϕ, *dϕ/dt*, pressure, water level, etc.). EDF decided that the benefits of the change in terms of safety would be limited.

Determination of variables LPD and DNBR in 1300 MWe and 1450 MWe reactors takes into account reactor thermal power (*Pth*) and the radial form factors *Fxy*(*z*) obtained either from the neutron flux maps produced using the in-core instrumentation system in the configuration where all the RCCAs are withdrawn, or from calculations made for each refuelling operation in various symmetrical RCCA insertion configurations. The axial power distribution *P*(*z*) is also taken into account, determined from measurements made by four multistage detectors located in shafts positioned around the vessel. Each of these detectors, comprising six 10-cm active sections, is shielded by cadmium and polyethylene to ensure that only neutrons arriving directly from the core, without being reflected, are measured. In 1984, during startup tests on Paluel Unit 1, the first-off unit of the 1300 MWe (P4) reactor series, 160 flux maps were produced using the in-core instrumentation system, with different control RCCA insertion configurations, recording the electrical currents delivered at the output of the multistage external detectors for each configuration. These measurements confirmed that the in-core axial power distribution could be established with sufficient accuracy from the measurements delivered by the multistage detectors located outside the vessel and that measurement uncertainty for these detectors could be quantified, in particular for definition of the reactor monitoring and protection thresholds.

For the EPR, SPND calibration and the method for determining variables LPD, DNBR and AO provide the local power variations without using the variables measured by the ex-core detectors, provided that the loss of representativeness of these measurements in certain configurations is taken into account.

Lastly, pressure in the containment is also one of the monitored variables that can trigger a reactor trip.

Table 5.5 at the end of this chapter shows for which variables mentioned above non-compliance with the associated criterion leads directly or indirectly[225] to triggering a reactor trip for the different incident and accident families (concepts defined in chapters 6 and 8) studied in a pressurized water reactor safety analysis report. For each type of incident or accident, the table shows the redundancy of the monitoring parameters that ensure reactor core protection.

Operating transient studies examine the changes in reactor operating parameters (core inlet and outlet water temperature, reactor coolant system pressure, etc.) over time, associated with the operating conditions defined for the reactor design (covered in Chapter 8). These studies serve as the basis for defining the threshold values for triggering the protection system or for checking that these values are appropriate.

[225] By the signal that triggers safety injection.

5.7. Using uranium and plutonium mixed oxide (MOX) fuel

The use of MOX fuel in pressurized water reactors results from the decision taken in France to adopt a partly-closed fuel cycle for these reactors so as to limit the accumulation of plutonium (uranium-238 produces plutonium-239 under the effect of fast neutrons) and to make use of a portion of the large amounts of depleted uranium generated by the uranium enrichment process required to manufacture UO_2 fuel.

Use of MOX fuel was authorized for 900 MWe reactors[226]. This involved a complete review of studies conducted in neutron physics, thermal-hydraulics and safety.

On average, MOX fuel contains between 8 and 9% plutonium by mass (the term 'content' is used), including 4 to 5% fissile material, i.e. mainly[227] plutonium-239. One-third of the core consists of MOX fuel assemblies, which are arranged in the core so as to obtain uniform power distribution across the core. To limit excess power at certain points in the peripheral rods of UO_2 assemblies adjacent to MOX fuel assemblies, the rods in the latter do not all have the same plutonium content: the four corner rods have the lowest content, those on the four sides have a higher content, and all the others have the highest content (these are referred to as 'three-zone' assemblies).

Compared with a core loaded with UO_2 fuel, the use of MOX fuel assemblies (with the characteristics described above) results in:

– significantly 'harder' neutron flux (due to a larger number of fast neutrons);

– a lower fraction of delayed neutrons (about 450 to 510 pcm, instead of 500 to 700 pcm for a core loaded with UO_2 fuel assemblies only);

– a diminished xenon effect;

– roughly the same Doppler effect[228];

– a slightly greater moderator effect;

– reduced effectiveness of the thermal neutron absorbers (RCCAs and soluble boron);

– higher decay heat more than ten or so hours after shutdown (some fifteen per cent higher one day after reactor shutdown, about forty per cent after a week). However, in the first ten hours after a shutdown, decay heat of a MOX fuel assembly is about 5% lower than that of a UO_2 fuel assembly.

Moreover, the energy released by a fission of plutonium-239 is about 210 MeV, compared with about 200 MeV for a fission of uranium-235.

[226] Use of MOX fuel in 1300 MWe reactors will be considered by EDF during their fourth ten-yearly outage.

[227] More precisely, plutonium isotopes 239 and 241.

[228] Slightly more negative because plutonium-240 has greater absorption resonances.

MOX fuel is much more radioactive and radiotoxic[229] than enriched uranium fuel. Its fabrication, transport and use in a nuclear reactor consequently require increased radiation protection measures.

The use of MOX fuel began in 1987 in the 900 MWe Unit B1 of the Saint-Laurent-des-Eaux nuclear power plant. Restart testing of the reactor with its first load containing 16 MOX fuel assemblies included zero-power physics tests, flux maps at 5% nominal power and measurements taken to determine the efficiency of MOX-based assembly RCCAs. These tests aimed to confirm the predictions of the neutron physics calculations, and consequently the calculation methods, uncertainties, and how they were taken into account. Flux maps obtained at nominal power were then analysed. Gaps appeared between measurements and calculations and were wider at low power; calculation uncertainties were consequently revised upward compared with those adopted for UO_2 cores. The restart tests detected a power tilt of about 9% at low power and 2% in operation, which was taken into account in the safety studies.

[229] In terms of alpha and beta radiation emission.

Table 5.5. Values for which non-compliance with the associated criterion leads directly or indirectly to triggering a reactor trip for certain incident and accident families in the pressurized water reactor safety studies (case study for 1300 MWe reactors) – *(*) indicates the safety injection signal*.

	Reduction of neutron absorption in the core	**Excessive neutron moderation by secondary system depressurization**	**Reactor coolant system depressurization**	**Flow rate reduction in reactor coolant system**	**Heat sink fault**
	- Uncontrolled RCCA withdrawal - RCCA ejection - Uncontrolled boric acid dilution	- Inadvertent opening of an SG relief valve - Steam line break (SLB)	- Inadvertent opening of a pressurizer relief valve - Loss of coolant accident (LOCA) - SG tube rupture (SGTR)	- Partial loss of reactor coolant flow - Reactor coolant pump rotor blocked - Loss of off-site power (LOOP)	- Loss of feedwater to SGs - SG feedwater pipe break - Total loss of feedwater to SGs
- High neutron flux - Rapid flux variation	X X				
- High linear power density	X	X			
- Low DNBR	X	X	X	X	X
- Very low water temperature in the reactor coolant system cold legs		X (*)			
- High water level in the pressurizer					X
Pressurizer pressure: - low - very high		X	X		X
- Low flow rate in reactor coolant system - Low rotation speed on reactor coolant pumps				X X	
- Low SG feedwater flow rate					X
SG water level: - very high - very low			X		X
- Low steam pressure in secondary system		X (*)			
- High pressure in containment structure		X (*)	X (*)		

(*) Safety injection signal

Videos available for viewing

The Alchemists’ Crucible

Three Generations
of French Nuclear Power Reactors

Chapter 6
General Objectives, Principles and Basic Concepts of the Safety Approach

This chapter, like most of the following chapters, focuses on the types of pressurized water reactor (PWR) operated in France; the principles and concepts applied regarding safety, however, have a more general scope. French PWRs were originally developed by Framatome under licence from the US company Westinghouse. The French reactor manufacturer has gradually freed itself from the terms of the licence, first with the N4 series reactors, then with the European Pressurized water Reactor (EPR), a French-German design that incorporates significant changes from the previous reactors. Some technical details and the location and date of first criticality of the French nuclear power reactors are given in the appendix to this chapter.

In France, Nuclear safety is defined in Article L.591-1 of the Environment Code as "all the technical provisions and organizational measures related to the design, construction, operation, shutdown and decommissioning of basic nuclear installations, as well as the transport of radioactive materials, which are adopted with a view to preventing accidents or limiting their effects." In a broader sense[230], the technical and organizational provisions for ensuring normal operation of the facilities without

[230] *Analyse de la sûreté des installations nucléaires – Principes et pratiques* (Safety Analysis of Nuclear Facilities – Principles and Practices), Daniel Quéniart, *Techniques de l'ingénieur*, article BN3810 V1, July 2017.

excessive discharge of radioactive effluents and without excessive exposure of personnel to ionizing radiation can be associated with the above definition.

The corresponding principles and basic concepts, inseparable from the development of nuclear facilities by designers and operators, have been enhanced over time as knowledge has improved, not only through research work in the field of pressurized water reactor safety, but also through operating experience feedback from incidents and accidents.

6.1. General approach to risks – General objectives

Assessment of the risks involved in operating a nuclear facility leads to distinguish the potential risks of the possible harmful effects of the radioactive substances[231] in the facility and the energies capable of dispersing them within the facility or in the environment, from risks qualified as residual, i.e. risks that remain after taking into account the technical provisions and organizational measures taken with regard to nuclear safety (in its broadened sense).

Potential radiological risks must be identified on the basis of the nature and quantity of radioactive substances in the facility and their respective hazardous characteristics.

The general safety approach consists in 'processing' potential risks in such a way that residual risks become acceptable, as they cannot generally be reduced to zero.

The notion of probability is introduced naturally into this general safety approach, which aims to produce a double assessment of the situations that could result from facility operation in terms of both probability and severity of the consequences. It is generally accepted that the probability of an accident must be lower when the severity of its consequences for people or the environment is high. This is restated in ASN Guide No. 22 pertaining to the design of pressurized water reactors, produced by the French Nuclear Safety Authority (ASN) jointly with IRSN and published in July 2017: "One objective to be achieved consists in preventing radiological incidents and accidents and mitigating the consequences of those that might occur despite the implemented prevention measures; the consequences must be less severe as the estimated frequency of an incident or accident rises."

This general objective has significantly guided work in the safety field over the last few decades. In the early 1970s, the use of a risk matrix was suggested to distinguish an acceptable (authorized) domain from an unacceptable (prohibited) domain, the consequences being expressed in terms of radioactive iodine release, for example. One of the schematic representations of such an approach, the Farmer diagram[232], is shown in Figure 6.1. As stated in the introduction to this publication, the notion

[231] In addition to other risks (chemical risks, for example) that may exist within the facilities, which must be dealt with in the appropriate framework (in the name of 'protected interests' as defined in French regulations), but are not covered in this publication.

[232] Frank Reginald Farmer (1914-2001) worked at the United Kingdom Atomic Energy Authority and was later a professor at Imperial College London.

of acceptability has a political character and changes over time. What was judged acceptable when starting up the first units of the French nuclear power programme was no longer acceptable in designing the EPR. Between these two extremes there have been successive improvements and, furthermore, periodic reviews of reactors in operation have provided the opportunity to reinforce reactor safety in light of the most recent developments in nuclear safety. This applies in particular to the improvements judged necessary to extend operation of the 900 MWe units beyond their fourth ten-yearly inspection programme.

Nuclear power plant designers have implemented the general approach outlined above in a quantitative manner by coupling estimated frequency ranges with maximum permissible radiological consequences in order to obtain 'decoupling' values that served as a basis for designing the various components of nuclear power plants. Nevertheless, there could be no claim that this provided sufficient substantiation for a safety demonstration, a point developed in Section 8.7.3.

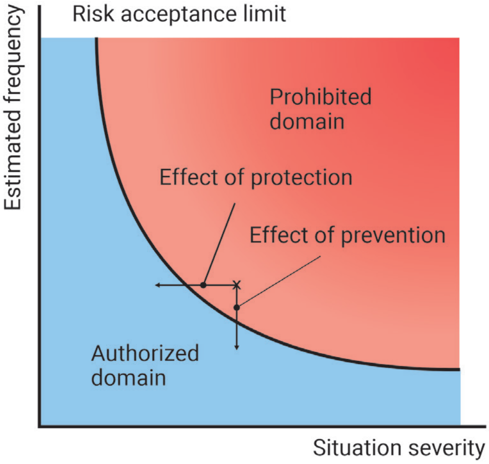


Figure 6.1. A theoretical schematic representation (Farmer curve) of the conceptual relationship between estimated frequency and situation severity. IRSN.

It should be emphasized that this nuclear safety reference is not in contradiction with the fact that it is based principally on a deterministic approach, in which a situation must be dealt with when it is considered plausible; design choices must provide sufficient mitigation of the situation. The deterministic approach is in any case complemented by the probabilistic approach, which provides an understanding of the risks associated with more complex situations and is used to define additional measures when necessary. These topics will be covered in further detail in Section 6.7.

European Directive 2014/87/Euratom of the European Council of 8 July 2014 – previously cited in Section 2.5.a) – amending EU directive 2009/71/Euratom[233],

[233] Directive establishing a Community framework for the nuclear safety of nuclear facilities.

has established at a political level the general nuclear safety objective for nuclear facilities: "that nuclear facilities are designed, sited, constructed, commissioned, operated and delicensed with the objective of preventing accidents and, should an accident occur, providing appropriate mitigation to avoid:

- early radioactive releases that would require off-site emergency measures but with insufficient time to implement them;
- large radioactive releases requiring protective measures that could not be limited in area or time."[234]

This objective, set out in ASN Guide No. 22 cited above, is in line with the objectives previously defined in the ASN's Technical Directives for the Design and Construction of the Next Generation of Nuclear Pressurized Water Reactors (*Directives techniques pour la conception et la construction de la prochaine génération de réacteurs nucléaires à eau sous pression*[235]), adopted by the ASN Advisory Committee for Reactors (GPR) and German experts in 2000, after seven years of technical discussions, and notified to Électricité de France (EDF) by the ministers responsible for nuclear safety in 2004, then in documents produced by WENRA[236]. ASN Guide No. 22 covers aspects relating to facility design itself, which must be based on appropriate application of the defence-in-depth principle (refer to Section 6.4), as well as aspects relevant to the nuclear safety demonstration, which assumes that a specific design has been chosen (in practice, design studies and safety demonstration studies are conducted through an iterative process). The guide reviews a number of statutory requirements and puts forward recommendations. It states in particular that the design of a pressurized water reactor must aim to:

- "minimize the number of incidents and limit the risk of occurrence of accidents";
- "limit, in incidents or accidents, release of radioactive or hazardous substances, or hazardous effects, and their impact on people and the environment, to levels as low as reasonably achievable";
- "prevent or, failing that, limit radioactive release that may result from incidents or accidents, including accidents with fuel melt";

[234] It is also stipulated in this directive that Member States shall ensure that, within the national framework, the objective defined above:
  - "applies to nuclear facilities for which a construction licence is granted for the first time after 14 August 2014;
  - is used as a reference for the timely implementation of reasonably practicable safety improvements to existing nuclear installations, including in the framework of the periodic safety reviews as defined in Article 8c(b) [of the directive]".

[235] This topic is developed in greater detail in Chapter 18.

[236] Refer in particular to the WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010.

and that:

- "accidents with fuel melt likely to result in major radioactive release with kinetics that prevent timely implementation of the necessary population protection measures must be rendered physically impossible or, failing that, extremely improbable with a high confidence level;
- the population protection measures that would be necessary in the case of other accidents with fuel melt must be very limited in terms of surface area and duration (no permanent rehousing, no evacuation other than from the vicinity of the site, no long-term restriction of consumption of foodstuffs other than from the vicinity of the site). For this purpose, such accidents must not result in contamination of vast areas or pollution of habitats in the long term."

Going beyond the general approach to risks, thinking on nuclear safety has led to gradual implementation of a wide range of principles, concepts and methods, applicable at the design stage as well as in the construction or operation stages, which are described later in this chapter.

With the fundamental objective of avoiding the exposure of workers and members of the public and release of radioactive substances into the environment, the companies[237] involved adopted a number of principles, concepts and methods in cooperation with nuclear safety organizations and bodies that were gradually being established. In particular, these included the 'fundamental safety functions', the interposition of physical confinement 'barriers' between radioactive materials and the environment, methods of deterministic analysis of postulated events, probabilistic studies and others.

Although for the first units of the French nuclear power plant fleet, and within the framework of the Westinghouse licence, EDF and Framatome applied US rules and practices extensively – such as the ASME[238] design and construction code – French companies subsequently developed rules for the design[239] and manufacture of systems and components that were assigned requirement levels based on the safety function ensured by each system or component.

Industrial enterprises, technical safety organizations, regulatory bodies and other organizations in the countries engaged in the development of nuclear power reactors have contributed their experience and know-how to the preparation of various documents representing a consensus on requirements and good practices, issued at international level (in particular IAEA standards published from the 1970s onwards) and European level (WENRA documents published since 2000, aiming to promote an

[237] A reminder here that the construction of nuclear reactors (whether for research or power generation) began in the mid-20th century in a few countries (including the USA, the Soviet Union, France and the UK) that were engaged in the research and development of technologies capable of using the energy produced by nuclear fission to generate electricity.

[238] American Society of Mechanical Engineers.

[239] Including the determination of facility characteristics in the design phase to satisfy criteria and regulatory practices.

achievable level of nuclear safety throughout Europe in spite of the diversity of situations in the various countries involved). These documents will be cited below where appropriate.

6.2. Fundamental safety functions

The specific nature of nuclear power reactors compared with other non-nuclear power facilities is the very large quantity of radioactive substances that they contain (Table 6.1). Personnel must be protected from these substances, as the dispersion[240] of even relatively small amounts in the environment could entail severe consequences for members of the public and for the environment.

The safety of these nuclear facilities consequently depends on adequate protection against sources of radiation and confinement of these sources.

If the sources are located in their designated locations, protection can be obtained by installing absorbent screens of appropriate materials and thicknesses, as discussed in Section 1.1.

Problems arise essentially from the possibility of dispersion of radioactive substances outside the designated locations. The potential causes of such dispersion must be identified in order to design the appropriate confinement.

Most of the radioactive substances contained in a nuclear power reactor (Table 6.1 below) are produced inside the fissile material (in the fuel pellets inside the metal cladding). The aim is to keep the substances where they are until the fuel can be processed in a reprocessing plant.

Table 6.1. Maximum radiological activity of some of the main fission products in a 900 MWe reactor at a maximum burnup rate of 33,000 MWd/tU (average per fuel assembly).

Fission products	Core, 2 h after shutdown	Reactor coolant system	Gaseous effluent
Noble gases	10^7 TBq[241]	3×10^2 TBq	2×10^2 TBq
Iodines	2×10^7 TBq	20 TBq	–
Caesiums	10^7 TBq	–	–

However, in normal conditions of use, to enable operation without refuelling for one year or longer and compensate various phenomena, a quantity of fissile material much greater than the cold 'critical mass'[242] must be available in the core. The power level of a reactor thus results from many parameter settings that must be controlled continuously.

[240] Dispersion or inadequate protection against radiation emitted by these substances.

[241] 1 TBq = 10^{12} Bq = 27 Ci (curie).

[242] Mass needed to sustain a chain reaction (see Chapter 5).

In accident conditions, the amount of energy released in a nuclear reactor can increase extremely fast and uncontrollably, and can only be limited by feedback[243] on temperature rises or fuel dispersion. **Management of the nuclear chain reaction**, also referred to as 'reactivity management or control', consequently takes on particular importance.

Moreover, as stated previously, significant energy release continues for a very long time after stopping the chain reaction, driven by the radioactivity of the nuclear fission products in the reactor core.

Each radioactive fission product releases this energy according to its own specific half-life, which may be very short (less than a second), average (months or years), or very long (hundreds or thousands of years, or even longer). The resulting decay heat decreases over time (an example of the time profile of power reactor decay heat is given in Section 5.3). It is far from negligible, and requires continuous cooling over long periods. **Decay or residual heat removal** is consequently a constant concern with regard to a nuclear reactor, whether in operation or shut down.

The specific characteristics summarized here underlie the three **fundamental safety functions**[244] for the protection of people and the environment:

- **control of nuclear chain reactions**,
- **removal of heat** produced by radioactive substances and nuclear reactions,
- **confinement of radioactive substances**, most of which are located in the fuel, but which are also found in the reactor coolant or in the spent fuel pool water, in the reactor building, the fuel building, or even in other spaces inside the facility.

French regulations[245] define another fundamental safety function: the **protection of people and the environment against ionizing radiation**, which includes worker radiation protection.

6.3. Confinement barriers

When the decision was taken in France to abandon the UNGG[246] reactor type (gas-cooled reactors) after the last one built, Bugey Unit 1, and to build pressurized water reactors under US licence, various major nuclear facilities of all-French design had already been built or were under construction (UNGG reactors, research reactors, RAPSODIE and PHENIX fast-neutron reactors, etc.). The safety approach developed in France at the time was based on placing physical barriers between radioactive substances on one hand, and people and the environment on the other. This was the approach used at first for pressurized water reactors. The concept of 'defence in depth',

[243] See Section 5.2.

[244] Fundamental Safety Functions are also referred to as 'Basic Safety Functions' or 'Main Safety Functions' in IAEA standards.

[245] Order of 7 February 2012, I, Article 3.4.

[246] *Uranium naturel-graphite-gaz*, i.e. natural uranium, gas graphite.

which originated in the USA, was subsequently adopted by French operators and safety organizations and adapted to take into account their experience.

Jean Bourgeois, who will be the first director of the *Institut de protection et de sûreté nucléaire* (Institute for Protection and Nuclear Safety) established at CEA in 1976, described the barrier safety approach in the following terms at a congress in Vittel in 1973:

"Protection of the public against the consequences of an accidental release of fission products rests on the interposition of a series of leaktight barriers. Safety analysis therefore consists firstly in ensuring the validity of each of these barriers and their correct operation under normal and accident reactor operating conditions.

This kind of analysis emphasizes the progressive nature of safety by distinguishing three successive but interrelated stages:

– **prevention**: the validity of each barrier must be demonstrated by the materials selected, as well as their suitability to operating conditions[247] and their ability to maintain the specified characteristics over a period of time. It is essential that the technological limits be shown so that the real margin between these limits and the operating conditions can be defined with a good degree of certainty;

– **monitoring**: designed to detect any drift within the margins defined above in order to be able, if necessary, to actuate a corrective action, either manually or automatically, in good time for return to normal operating conditions;

– **mitigating action**: if an accident occurs and technological limits are exceeded, the purpose of mitigating action is to prevent the release of radioactive substances or limit the amounts released.

For each type of reactor, there are generally three or four barriers [...] considered to be both leaktight and resistant: the fuel cladding, the reactor coolant pressure boundary, the primary containment and possibly the secondary containment. Each of these is examined in detail under the three operating conditions described below:

– <u>normal operation</u>: the simplest and best-defined category for which the fixing of margins with regard to technological limits must take into account any uncertainties which might exist;

– <u>normal operating transients</u> (startup, power build-up, load variations[248]): as a general rule, the safety margins fixed for normal operating conditions must allow these transients to be absorbed without tripping irreversible corrective actions;

– <u>abnormal operating transients</u>, following equipment failure or induced by human error: the drawing up of various possible sequences reveals critical points and hence enables improvement of reliability or monitoring processes.

[247] The concept of 'operating conditions' was relatively broad at that time and was subsequently developed in depth, resulting in the concept described in Chapter 8.

[248] Power supplied by the reactor.

In order to synthesize this survey of the barriers and particularly to determine their independence from each other, which is essential for safety assessment, an examination of the development of typical major accidents must be undertaken. This final process has a rather formal character as, in certain cases, it involves postulating events which cannot be precisely identified. This has the advantage of allowing assessment of the dynamic response of radioactive products to transfer from the core to the outside containment and of providing an order of magnitude for site radiological consequences if the integrity of all barriers were to be breached."

This approach is deterministic by nature, in that it involves investigating the potential consequences of a number of 'abnormal' (postulated) situations defined on the basis of predictable failures of the fundamental safety functions, without examining the sequence of events that could lead to each situation.

Definition of the confinement barriers depends greatly on the technology of the reactor under study and the associated parts of the facility. The confinement barriers for the radioactive substances in the core of pressurized water reactors are identified in figures 6.2 and 6.3. Moreover, even for a given reactor, although the definition of the first barrier is straightforward[249] (all the cladding on fuel rods), defining the other barriers specifically can be problematic[250].

The second confinement barrier is formed by the boundary of the reactor coolant system, in which the reactor core coolant circulates, inside the reactor building. However, there are ancillary systems where the coolant circulates in buildings other than the reactor building, including in accident situations. These specific aspects must be taken into account.

The third confinement barrier is associated with the reactor building (also called the 'containment'), including wall penetrations and their isolation systems. The boundary of the secondary system inside the reactor building and the boundaries of the steam generators are also part of the limits of the third barrier. This also applies to the steam generator tubes, as explained in the next section. However, the third confinement barrier is complex above all because of the specific aspect mentioned above: in an incident or accident situation, certain systems required to control the incident or accident convey radioactive fluid (reactor coolant or air in the containment) outside the containment itself, and this must be taken into account. The boundaries of these systems thus form part of the third confinement barrier (this is generally referred to as 'extension of the third confinement barrier').

[249] It should nevertheless be noted that in some documents, for example from the IAEA, the fuel matrix is sometimes identified as the first confinement barrier. That definition has not been adopted in France, although the fuel matrix does provide some confinement of fission products in certain low-severity conditions. However, the structure of the fuel pellets changes under irradiation (cracks appear) and 'leaktightness' of the pellets cannot be monitored during reactor operation.

[250] Confinement barriers for spent fuel pools are based technically on mechanisms substantially different from what follows (see Chapter 15).

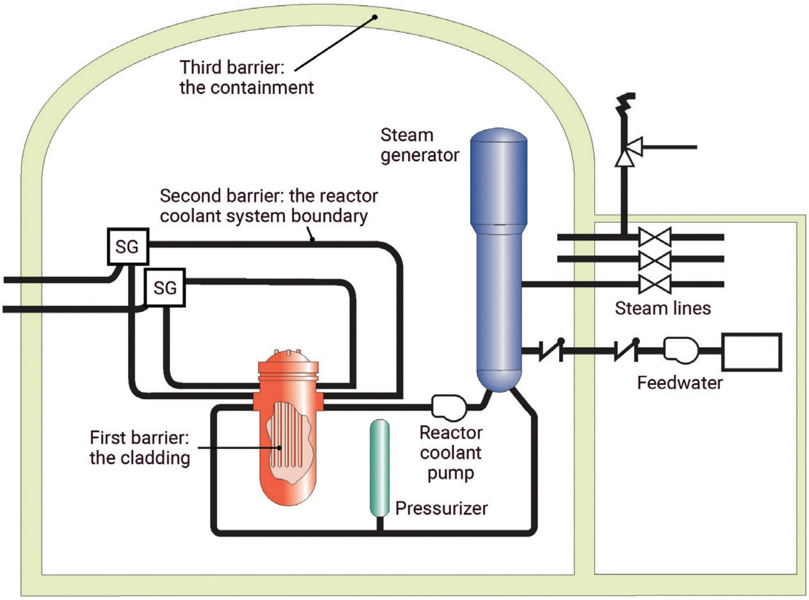


Figure 6.2. Confinement barriers of a pressurized water reactor. Georges Goué/IRSN.

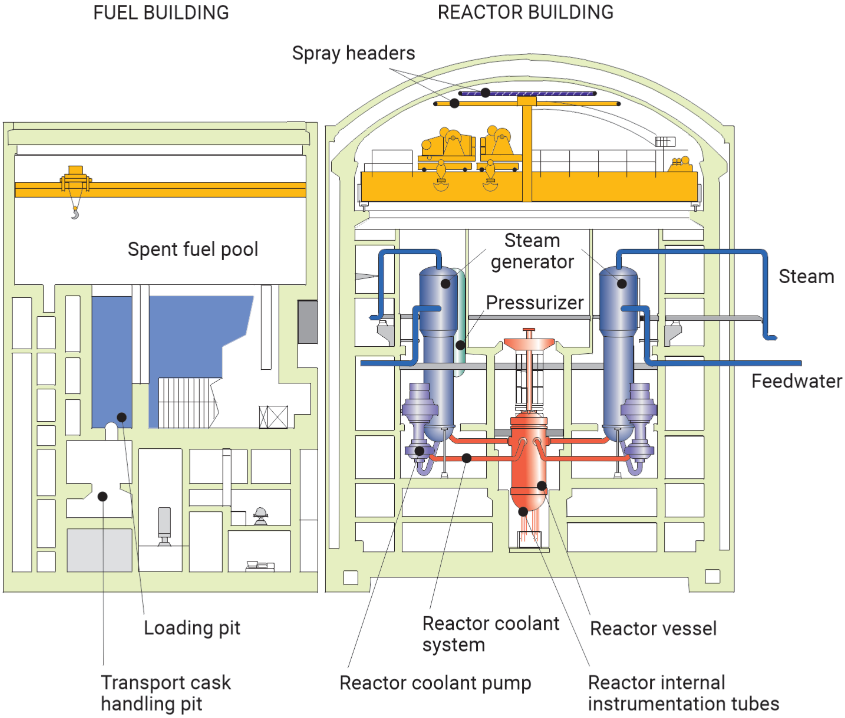


Figure 6.3. Partial section of a P'4 series 1300 MWe reactor, with double containment. IRSN.

The pressurized water reactor has a singular feature: the steam generator tubes. Their total surface area is more than a hectare (2.5 acres), and their walls are very thin, about one millimetre. Given the relief valves and letdown valves of the secondary systems outside the containment, the steam generator tubes form part of both the second and the third confinement barriers. The design-basis pressure of the secondary system is lower than that of the reactor coolant system, so, in the event of a steam generator tube rupture, a pressure increase in the part of the secondary system involved may lead to opening of secondary system valves located outside the reactor building, upstream of the isolation valves, and to release of radioactive substances into the atmosphere. This topic is discussed further in Chapter 10.

The above remarks were taken into account in development of the defence-in-depth concept, which includes the confinement barriers.

6.4. Defence in depth

Defence in depth is a concept[251] providing a general framework for an approach to ensuring facility safety in the design phase and during operation, also applied to the associated safety analyses[252]. Although developed in the 1960s in the USA, it was structured more precisely in the 1990s on the basis of nuclear safety practices and measures already in place in various countries, up to and including plans for dealing with emergency situations.

The barrier approach in terms of prevention, monitoring and mitigation is included in the defence-in-depth approach, but as part of a broader approach considering all the systems, structures and components[253] that have an influence on safety, along with the human and organizational measures that also affect safety.

The defence-in-depth concept is based on[254] the general idea that, although measures must be taken to avoid incidents or accidents as much as possible, it should nevertheless be postulated that some may occur. Means of mitigation must therefore be studied and the appropriate measures implemented.

Implementation of "a defence-in-depth concept [...] centred on several levels of protection, including successive barriers preventing the release of radioactive material

[251] The term 'strategy' is also used, in particular in IAEA documents.

[252] Defence in depth is a very general concept. A defence-in-depth approach can be adopted with regard to the risks of fire and explosion in nuclear facilities (see sections 11.6 and 11.7). In Chapter 22, in which a number of 'significant events' (concept defined in Section 22.2) that have occurred during maintenance operations are discussed, it is also noted that a defence-in-depth approach is necessary for the safety of operating activities – consistent with paragraph 71 on this subject in the INSAG-10 report.

[253] Structures, Systems and Components (SSC) in the IAEA standards.

[254] For further information on the historical development of defence in depth, refer to Section 03.1 of the WENRA report entitled Safety of New NPP Designs – Study by Reactor Harmonization Working Group RHWG, March 2013.

to the environment" was recommended as early as 1988 in the INSAG-3[255] document entitled *Basic Safety Principles for Nuclear Power Plants*, a report by the International Nuclear Safety Advisory Group (INSAG) of the IAEA, with the following objectives:

- "to compensate for potential human and mechanical failures,
- to maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves,
- to protect the public and the environment from harm in the event that these barriers are not fully effective."

This leads to applying a deterministic approach to study various postulated situations of increasing severity, in order to be ready to cope with them in the best possible conditions.

The defence-in-depth concept is translated into technical, human and organizational measures, grouped in levels, each of which sets out to avert damage likely to result in involvement of the next level and to mitigate failure of the previous level. This requires making sure that the levels are sufficiently independent.

The defence-in-depth concept has been enriched over time, resulting in the adoption of five levels, defined in the INSAG-10 report entitled *Defence in Depth in Nuclear Safety*, published in 1996. This report is used below as the basis for describing defence in depth. Some information relating to levels 3 and 4 has changed since the publication of INSAG-10, and are discussed in Section 6.4.1, given their importance for the safety analysis.

It is of course essential that the defence-in-depth measures considered in the reactor design phase remain effective after it has been built and throughout its operating lifetime.

6.4.1. Levels of defence in depth

Organizing defence in depth in five levels[256], as recommended by the INSAG-10 report, has been accepted and adopted internationally. The concept of 'level' corresponds to a set of measures covering intrinsic characteristics of the facility in question, equipment (systems, structures and components), operating procedures, and organizational measures (for the management of emergency situations, for example).

Even though implementation of defence-in-depth levels may differ from country to country and may to a certain degree depend on plant design, the main principles are always the same.

Level 1, the first level, is predominately a prevention function. Level 5, the last level, involves mitigation, i.e. limiting the radiological consequences of an incident or accident to protect the public and the environment.

[255] Reproduced in the 1999 revised version INSAG-12.

[256] The term 'level' is used in this context, instead of 'line of defence' used in particular in an approach implemented in the safety analysis of other reactor types.

Application of the general concept of defence in depth as set out above has some limitations, discussed in the INSAG-10 report (Paragraph 28): “If it is not feasible to have independent levels of defence against some events (such as sudden reactor pressure vessel failure), several levels of precautions are introduced into the design and operation. Such precautions may be taken, for instance, in the selection of materials, in periodic inspection or in siting, or in design by incorporating additional margins of safety.” This topic is discussed further in Section 8.2.2.

The levels are described below.

▶ Level 1: prevention of abnormal operation and failures

This involves ensuring that the plant is intrinsically robust with respect to the potential failures and hazards defined in the design phase. This means that once the initial definition of the facility design (selection of the design options) is complete, the normal and abnormal conditions of operation should be clearly identified (as exhaustively as possible), and that appropriate margins should be adopted in designing systems and components so that they are sufficiently robust and resistant.

Furthermore, Level 1 provides the initial basis for protection against external and internal hazards (earthquake, aeroplane crash, fire, blast wave, flooding, etc.), even though some additional protection may be required at higher levels of defence. The choice of site obviously plays a key role in limiting these constraints.

The materials used for equipment (systems, structures and components) must be selected carefully, the fabrication processes must be qualified, and the technologies used proven by operating experience feedback. Application of appropriate standards[257] (by defining the conditions of design, procurement, manufacturing and manufacturing inspection of equipment important for facility safety, for example) contributes to equipment robustness.

Moreover, the intrinsic characteristics of a given reactor technology[258] (in terms of neutron feedback, thermal inertia, etc.), the design of the human-machine interface, the level of automation and the time available before manual intervention is required can make a major contribution to safety. Note that the examples of intrinsic characteristics mentioned here generally contribute to preserving the next levels. This obviously does not compromise the objective of independence between levels mentioned previously, and featuring these characteristics at different levels should be encouraged.

The choice of personnel involved at each stage in facility lifetime (design, equipment manufacture and facility construction, inspection and testing, operation – including shutdown states), their training, the measures implemented by the different bodies

[257] For the design and manufacture of mechanical equipment, the relevant American ASME code, or the RCC-M code for French pressurized water reactors, are relevant examples.

[258] Designers often use the term ‘process’ to refer to the overall technology of a facility such as a nuclear reactor.

involved (designer, operator and their contractors) with regard to quality assurance and safety culture[259], the clear definition of responsibilities as well as the clarity of the operating procedures, all contribute to the prevention of failures throughout facility lifetime.

Methodically taking into account operating experience feedback is also a key element that helps to reinforce prevention of facility failures.

▶ Level 2: control of abnormal operation and detection of failures

As it is not possible to completely avoid situations where the facility leaves its normal operating domain, the second level is based on systems designed according to specific criteria (redundancy, qualification, etc.) capable of stopping an abnormal deviation[260] and bringing the facility back to its normal operating domain.

Checking that the facility complies with design assumptions by conducting in-service inspections and periodic equipment tests can detect any degradation that has occurred – despite preventive maintenance measures taken – before it affects facility safety[261].

Systems that measure the radioactivity in the different fluids and monitor the atmosphere in various spaces are used to check that confinement barriers remain leaktight. Specific tests are conducted to check that purification systems are effective.

Systems for reporting and providing clear information in the control room with regard to faults and the state or configuration of facility structures, systems and components make it easier for operating personnel to deal with faults within an appropriate time frame.

Automatic systems used to control the 'process' (and send warnings to operators in the control room) are set into operation in order to correct any drifting in certain reactor parameters (power, pressure and temperature limitation systems[262], motor-driven relief valves, etc.), to interrupt an undesired phenomenon that cannot be sufficiently controlled through control systems[263] or to compensate for unavailable sources; if necessary, the reactor may even be shut down[264].

[259] Concept developed following the Chernobyl nuclear power plant accident (see Chapter 4).

[260] In the sense covered by the notion 'anticipated operational occurrences', according to the terminology adopted in IAEA documents, corresponding to predictable events (incidents).

[261] For French PWRs, in-service equipment monitoring is covered by RSE-M (equipment in-service monitoring rules), published by AFCEN (*Association Française pour les règles de conception, de construction et de surveillance en exploitation des matériels des chaudières électronucléaires*, a French association that defines the rules governing design, construction and in-service monitoring of nuclear power plant components and equipment).

[262] The EPR has this type of limitation system, which, for example, drops a certain number of RCCAs in the event of a reactor coolant pump failure to adjust core power in function of coolant flow.

[263] It may be considered that control systems whose functions are to compensate nuclear fuel burning in the core and adapt reactor power to the electrical power demand (predictable and normal phenomena) belong to Level 1 of the defence-in-depth approach.

[264] In the INSAG-10 report, the protection system (reactor trip) is assigned to Level 2 in Table 1 and Level 3 in the text.

▶ Level 3: control of accidents within the design basis

The first two levels of defence in depth are designed to avoid the occurrence of accidents.

Despite the attention given to these two levels, postulated accidents may occur; for example, a pipe supplying coolant to the core (i.e. to the reactor coolant system) could break. Postulated accidents are assessed using a deterministic approach. This is one of the major components of facility design and the corresponding safety demonstration. Postulated accidents serve as the basis for the design of 'engineered safety features'[265], which, associated with the protection system, avert severe core damage (such as core melt). The accidents to be studied and the associated criteria must be selected early in the design phase.

These dedicated systems thus have no role in normal operation of the facility. They may be activated automatically, since, whatever the circumstances, human intervention cannot occur in a timely manner, given that sufficient time must be taken for operators to establish well-founded diagnostics. Proper operation of these systems in the postulated accident situations prevents any impact on the structural integrity of the core, so it can be cooled subsequently. Release to the environment is thus very limited (due particularly to isolation of the containment).

The systems in a French pressurized water reactor that can be activated at the third level of defence in depth include:

- the protection system, which triggers reactor trip (RT) if thermal-hydraulic or neutron thresholds are exceeded (they are set to protect the core in the postulated accident situations);
- the steam generator Emergency FeedWater System (EFWS), which circulates water on the secondary side of the steam generators to cool the reactor coolant system water if the steam generator Main FeedWater System (MFWS) is unavailable[266]. The EFWS draws water from a dedicated tank and conveys it to the steam generators using motor-driven pumps powered by emergency-supplied electrical switchboards, or turbine-driven pumps powered by steam take-off from the steam lines, avoiding the need for electrical power;
- the Safety Injection System (SIS), which injects borated water into the reactor coolant system in order to restore sufficient water inventory in the core and

[265] Or 'engineered safety systems'. 'Engineered safety features' is the term used in the INSAG-10 report.

[266] Especially in accident situations such as loss of off-site power, a steam generator main feedwater system pipe break or a steam line break. However, it should be noted that, in French reactors other than the EPR, this system also has a role in normal reactor operation, in place of the MFWS, i.e. filling the steam generators after a reactor refuelling outage, supplying water to the steam generators during transitions from hot shutdown to connection of the closed-loop residual heat removal system (RHRS) and, conversely, supplying water to the steam generators after RHRS disconnection until hot shutdown.

ensure core cooling. It comprises various subsystems that inject water at different pressures[267]. In French nuclear power reactors up to and including the N4 series, borated water is drawn first from the refuelling water storage tank of the Fuel Pool Cooling and Purification System (FPCPS)[268], then eventually, in the containment water spray and recirculation phase, from the containment sumps; the changeover is automatic. In the EPR, borated water is drawn directly from the In-Containment Refuelling Water Storage Tank (IRWST) – see Section 18.2.3;

– the Containment Spray System (CSS) in the containment, which lowers the pressure in the containment in the event of an accident resulting in a significant pressure increase in the reactor building (for example, a loss-of-coolant accident or core melt in the 900 MWe, 1300 MWe and 1450 MWe reactors, or core melt in the EPR only), thereby preserving containment leaktightness. The CSS also reduces radionuclides released in aerosol form in the containment. CSS water is drawn first from the FPCPS tank then, in the containment water recirculation phase, from the containment bottom sumps.

As in the case for Level 2 measures, to ensure adequate reliability of the engineered safety features, special attention must be given to their potential failures, whence the application of rules or principles such as redundancy, spatial separation, and diversification (see Chapter 7, which presents a few generic safety options available in the design phase). Engineered safety systems must also undergo periodic testing, as well as appropriate in-service monitoring and maintenance. Special attention must be given to the procedures used to qualify[269] these systems for accident conditions, which obviously cannot be done by triggering accidents in the facility itself.

▶ Level 4: control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents

The core-melt accident on Unit 2 at the Three Mile Island nuclear power plant in 1979 (see Chapter 32) prompted efforts to develop the means to cope with plant situations that were not covered by the first three levels of defence in depth and that could lead to severe core damage[270]. The broad aim of the fourth level of defence in depth is to ensure that the likelihood of an accident entailing severe core damage, and the magnitude of radioactive release in such a case, are both kept as low as reasonably

[267] 'Low-head' and 'medium-head' injection systems, with a 'high-head' system for the 900 MWe reactors.

[268] The FPCPS removes decay heat from the fuel assemblies stored in the spent fuel pool, among other functions.

[269] Qualification, which may be based on testing and inspections, is the process that aims to demonstrate that an equipment item as designed and manufactured is fit to meet its purpose in accident conditions. This topic is also approached in Chapter 7 (Section 7.4.3), and in Chapter 19 on startup testing.

[270] Situations often designated as 'severe accidents'.

achievable, while taking into account economic and social factors. To achieve this objective, measures need to be taken not only to prevent severe core damage, but also to gain time before it becomes necessary to take measures to protect the off-site population. In this case it is essential to maintain the confinement function under the best possible conditions.

On-site accident management must aim to avoid the need to apply off-site protection measures (especially population protection). Organizational measures such as on-site emergency plans and personnel preparation and training for accident situations are also necessary.

The introduction of measures for controlling severe accidents should not, of course, be used to compensate deficiencies at the previous levels of defence in depth.

In a French pressurized water reactor, the following technical measures are designed to mitigate core-melt situations:

– for reactors other than the EPR, the containment spray system (CSS) mentioned above, and the deliberate containment venting system[271] associated with operating procedure U5; in core-melt situations, this venting system limits pressure in the containment (to avoid containment damage), while filtering any release of radioactive substances into the environment;

– the autocatalytic hydrogen recombiners, used to avoid explosion of hydrogen inside the containment;

– for the EPR, the core catcher located at the bottom of the containment, and the containment heat removal system (CHRS) in the reactor building – which also features a containment water spray system.

Further details of these three measures are given in Chapter 17.

At Level 4 of defence in depth, and as formulated in the INSAG-10 report of 1996, consideration must be given to severe plant conditions that were not explicitly addressed in the original design (levels 1 to 3) of currently operating plants owing to the very low probability that they could occur. Such plant conditions may be caused by multiple failures, such as the complete loss of all trains[272] of a safety system, or by an extremely unlikely event such as a severe flood. Some of these conditions could potentially result in the release of radioactive substances to the environment. The thermal inertia of the plant provides time to deal with some of these conditions by means of additional measures and procedures (systems and components, operating procedures)[273].

[271] This would obviously only be implemented in cooperation with public authorities.

[272] The term ‘line’ is also used.

[273] It should be noted that, for the EPR, activation of the CHRS is envisaged in certain multiple-failure situations, such as a small-break loss-of-coolant accident (SB LOCA) combined with total loss of low-head safety injection (LHSI).

For French pressurized water reactors, the control measures associated with H and U situations may also be applied (see chapters 13, 17 and 33).

▶ Level 5: mitigation of the radiological consequences of significant releases of radioactive materials

If the previous measures have failed or have not proven sufficiently effective, application of off-site protection measures must be considered (i.e. collection and evaluation of data on radiological exposure levels, protection measures such as sheltering or even evacuation of the population, ingestion of stable iodine and prohibition of consumption or marketing of foodstuffs). Implementation of these measures is prepared by public authorities. The decision to apply these measures is based on analyses of the situation by the operator and the safety organizations and on environmental radioactivity measurements.

These measures are defined in the off-site emergency plans discussed in Chapter 38.

Periodic exercises are conducted to check and, if necessary, improve the measures planned to respond to emergency situations.

▶ Documents issued after publication of the INSAG-10 report

For reactor generations built after publication of the INSAG-10 report in 1996, the report already clearly indicated the benefits of considering events resulting from multiple failures as belonging to Level 3 of defence in depth rather than Level 4[274].

In Europe, in a report issued by the Reactor Harmonization Working Group (RHWG) in 2013 on new reactor designs[275], WENRA introduced some changes in the definition of the defence-in-depth levels and sought to associate these levels with the event categories considered in the deterministic safety analysis (normal operation, incidents, accidents), as defined in Section 6.5 below. To strengthen preventive measures against severe core damage, it was considered that the means provided to prevent and control events caused by postulated multiple failures needed to be reinforced. In the RHWG report mentioned above and, in France, in ASN Guide No. 22, these events are now considered as Level 3 of defence in depth (which pertains to Level 3b operating conditions).

[274] Moreover, the defence-in-depth concept described in the 1996 INSAG-10 report was subsequently defined in greater detail. For example, in 2005, the IAEA published the document Assessment of Defence in Depth for Nuclear Power Plants (Safety Reports Series No. 46), as a guide to assessment of the robustness of defence in depth in the case of a facility such as a nuclear power reactor.

[275] RHWG report entitled Safety of New NPP Designs – Study by Reactor Harmonization Working Group (RHWG), March 2013.

6.4.2. Elements common to the different levels of defence in depth

Human and organizational factor aspects must be taken into account at all levels of defence in depth.

Defence in depth also assumes that the different levels are treated independently as much as possible. It is therefore very important to identify the events or failures that could affect several levels simultaneously (for example, when a particular failure might prevent the operation of means provided for failure mitigation), and to assess whether the measures taken are sufficient. Hazards are a particular risk in this respect, as by nature they can affect different levels of defence in depth simultaneously. This problem is discussed several times in later chapters. It is one of the particular points requiring special attention for new reactors, and for existing reactors when it is time for their periodic reviews.

Systems important to safety must be designed for high reliability. They are therefore governed by specific design, installation and maintenance rules. Effective implementation of defence in depth assumes that the measures taken at each level are defined according to an appropriate degree of conservatism.

Conservatism and safety margins are concepts applied specifically to the first three levels of defence in depth with regard to single initiating events occurring in the normal, incident and accident operating conditions covered in Chapter 8.

It is acceptable to apply conservatism less stringently when dealing with multiple failures and severe accidents (core melting, for example). Realistic estimates are also preferable for providing proper population protection in real-life release situations.

The Focus feature at the end of this chapter defines a certain number of concepts used for design and safety analysis purposes when applying conservatism in the broad sense.

6.5. Events considered: terminology adopted for nuclear power reactors

It is clear from the previous section that application of the defence-in-depth concept means studying a certain number of events, whether they are postulated because their occurrence during the facility lifetime appears inevitable or simply because it cannot reasonably be demonstrated that they are not plausible. This study is an important component, although not the only one, of the support documents substantiating the safety of a facility such as a nuclear reactor, in other words, its safety demonstration.

At this stage it is necessary to define certain terms used customarily and encountered frequently further on in this book.

In France, normal events are treated as Category 1 Operating Conditions, covering all normal operating states (including shutdowns), and also any transitions between these operating states (for example, reactor shutdown or startup transients).

The other events covered in the safety demonstration include (terminology specific to the EPR is given in Chapter 8):

- incidents[276], covered under Category 2 Operating Conditions, which are predictable events that may occur frequently (up to several times a year);
- accidents, of lower probability than incidents, covered under Category 3 and Category 4 Operating Conditions; Category 4 accidents are hypothetical accidents nevertheless taken into account for safety purposes.

These four operating condition categories constitute the 'design-basis domain' (consistent with the English term 'Design-Basis Accidents' [DBA]), or, in keeping with the more recent French designations (and adding internal and external hazards), the 'design reference domain' (ASN Guide No. 22).

The manner in which operating conditions are defined, i.e. based on the estimated frequency of initiating events, and the associated study methods are described in Chapter 8.

In addition to these operating conditions, initiated by single failures, other events, generally assuming multiple failures, must also be covered in the safety demonstration. They constitute a 'beyond-design-basis' framework – 'Beyond-Design-Basis Accidents' (BDBA)[277] – or, adding situations with core melt (and hazards), the 'Design Extension Conditions' (DEC) introduced in more recent documents issued by the IAEA[278], WENRA and in ASN Guide No. 22.

The study of multiple failures and situations with core melt (i.e. severe accidents) developed gradually in France from the mid-1970s, and was then reinforced after the accident in 1979 at the Three Mile Island nuclear power plant in the USA. Multiple failures are covered in Chapter 13 and situations with core melt are covered in Chapter 17.

In addition to all these considerations, internal and external hazards must also be taken into account. Chapters 11 and 12 discuss and illustrate how this is achieved in the reactor design phase.

[276] Anticipated Operational Occurrences.

[277] In France, the term 'complementary domain' for multiple-failure situations was originally used (see Chapter 13).

[278] IAEA document SSR-2/1, Safety of Nuclear Power Plants: Design, Revision 1 published in 2016, introduces the concept of 'Design Extension Conditions', which includes situations more severe than design-basis accidents, postulating additional failures and situations with fuel melt. Consequently, the study of such events must aim to determine whether the facility design (including the ultimate confinement barrier) can mitigate them adequately or whether reinforcement (of the ultimate barrier, for example) or the installation of additional systems (power supplies, 'ultimate' makeup water, etc.) should be envisaged.

6.6. WENRA reference levels

One of the objectives set by WENRA, the Western European Nuclear Regulators Association presented in Section 3.1.9, is to develop a common approach to nuclear safety within the European Union. With this in view, after its first studies on safety in Eastern European countries applying for European Union membership, it defined reference levels applicable to existing facilities throughout the EU. The reference levels, from WENRA's point of view, are the best nuclear safety practices reasonably applicable and should consequently be implemented in the WENRA member countries for any reactors in operation. The first version of the reference levels was published in 2006. WENRA itself does not have a regulatory role, so its members undertook to introduce the reference levels into the regulations of their respective countries to ensure that they were applied.

The reference levels were revised and updated in 2007 and 2008[279], respectively, then a new update was published in 2014, taking into account lessons learned from the Fukushima Daiichi nuclear power plant accident. All 341 reference levels are included in the WENRA report entitled Safety Reference Levels for Existing Reactors, published on 24 September 2014, organized according to 19 subject matters given in Table 6.2 at the end of this chapter[280].

Hereafter this book will refer to these reference levels when discussing certain topics.

6.7. Deterministic safety analysis and probabilistic safety assessments

As discussed above, both in the safety analyses of confinement barriers, initially applied to the first reactors built in France, and in the application of defence-in-depth principles, events (operating conditions and hazards) are postulated, and it must be shown that the risk associated with their calculated consequences is acceptable.

The study of these events constitutes what is usually called the 'deterministic safety approach'. In addition to this approach, after partial developments involving, for instance, the loss of redundant systems[281], more complete probabilistic safety

[279] WENRA Reactor Safety Reference Levels, Revision, 1 March 2007 and WENRA Reactor Safety Reference Levels, 1 January 2008.

[280] These reference levels involve nuclear safety and, to a certain degree, radiation protection. They do not cover aspects relating to security nor emergency response measures implemented by public authorities.

[281] In observance of SIN letter no. 1076/77 of 11 July 1977. For these early developments, see Section 14.1. Moreover, it is important to note that in the field of nuclear safety applied to reactors, the distinction between the deterministic approach and the probabilistic approach does not imply that using one invalidates the other: on many points the deterministic approach applies statistical or probabilistic considerations. For example, operating conditions are categorized on the basis of the estimated frequency of occurrence of initiating events, as discussed in Chapter 8.

assessments (PSA) were gradually developed for nuclear power reactors – from the early 1980s in France. They consist in using (speculative) analysis to determine which scenarios or sequences could potentially lead to core melt (Level 1 PSA), along with the associated probabilities, or subsequently the possible resulting categories of radioactive release (Level 2 PSA), also with the associated probabilities. For example, in the early 1990s, Level 1 PSAs confirmed that certain concerns about the risks of core melting in pressurized water reactor shutdown states were well founded. This is discussed further in Section 22.1.

A few 'assumptions' regarding the use of the deterministic approach or probabilistic approach for (PWR) power reactors are specified below.

The deterministic safety approach is used, for example, to:

- determine[282] or confirm the design basis for all equipment important to safety; the acceptability criteria and limits chosen for the design and operation of these equipment items must be satisfied;
- define or confirm the requirements that the equipment must satisfy, which will be taken into account during equipment qualification and operation;
- show that satisfactory control of incidents and accidents (within the 'design-basis domain' or 'design reference domain') can be achieved by combining automatic mitigating actions and prescribed operator actions;
- show that satisfactory control of accidents more severe than the design-basis accidents above (i.e. design extension conditions) can be achieved through safety measures combined with operator actions, taking into account the defined general safety objectives.

Probabilistic safety assessments must cover all reactor operating modes and reactor states, including shutdown states, with a special focus on:

- showing that a balanced design has been obtained (so that there is no particular point of the design or postulated event that would make an excessive contribution to the overall risk) and that defence-in-depth levels are as independent as reasonably achievable;
- ensuring that sufficient measures have been taken to prevent situations in which small deviations in facility parameters could entail large variations in facility performance (prevention of cliff-edge effects);
- assessing the results obtained, taking into account the safety objectives defined for the facility.

[282] This implies that the events (operating conditions and hazards) taken into consideration in the deterministic safety analysis lay the foundations for defining the 'design-basis situations' that serve to design (in particular, to size) facility structures, systems and components (a principle discussed further in Section 8.6).

In France, PSAs are governed by fundamental safety rule RFS 2002-01, published in December 2002, which describes acceptable methods for conducting Level 1 PSAs limited to internal events in the facility and also sets out the possible uses of such PSAs. Probabilistic safety assessments are covered in Chapter 14.

6.8. Lessons learned from the accident at the Fukushima Daiichi nuclear power plant on the concept of defence in depth and deterministic analysis

The Fukushima Daiichi nuclear power plant accident that occurred in March 2011 – described in Chapter 36 – led to the review of a number of general issues involving nuclear power reactor design, in particular the independence of defence-in-depth levels and facility robustness with regard to potential external hazards.

In France, as part of the complementary safety assessments requested by the Prime Minister (see Section 36.6), EDF conducted studies to assess the capacity of its facilities to withstand extreme hazards, more severe than those defined in the facility design phase (or those considered in the most recent facility periodic reviews). It was then decided to create the Nuclear Rapid Response Force (*Force d'action rapide nucléaire*, FARN) and install equipment sufficiently robust to withstand such hazards (forming a 'hardened safety core'), with the objective of not only preventing core melt as far as reasonably achievable, but also limiting the consequences should such a situation occur. The complementary safety assessments and the subsequent measures taken for the French nuclear power reactor fleet are discussed extensively in sections 36.6.5 and 36.6.6.

As stated above, the expression 'design extension conditions' has been introduced in the most recent documents on nuclear safety. ASN Guide No. 22 cited above, applicable to new reactor design, recommends in this context that "events more complex or more severe [...] than [those of the design reference domain] must be assessed in 'extended' design conditions so as to reinforce the capacity of the facility to deal with them, on the basis of an appropriate approach" with a particular focus on "external natural hazards of greater severity than those considered in the design reference domain." The study of such hazards aims to "ensure sufficient margins to achieve radiological objectives"[283].

[283] It should be noted that the WENRA report published in September 2014, updating the previously published safety reference levels for existing reactors in light of lessons learned from the Fukushima Daiichi nuclear power plant accident, includes a set of reference levels for natural hazards (Issue T – see Table 6.2). The report is more explicit than the IAEA SSR-2/1 safety standard discussed above with regard to taking into account hazards that are more severe than those considered in the 'design basis envelope', in the framework of 'design extension conditions'.

6.9. Safety culture – Quality control

For effective implementation of defence in depth, certain basic prerequisites are applicable to all the measures included in levels 1 to 5. These prerequisites include not only safety culture, a concept already extensively introduced in Chapter 4, but also quality assurance.

The principles and concepts set out above would have only a limited impact if quality was not fully assured, in the broad sense, for all activities involved in design, parts procurement, component manufacture, component installation, testing and inspection, preparation for operation, and all activities included in operation itself. It is of primary importance that the measures taken in the design phase remain effective or are improved throughout the operating lifetime of a facility. This entails the motivation of everyone involved and requires a dedicated organization.

EDF first approached quality assurance by organizing activities according to the following principles:

– write what we are going to do,

– do what we have written,

– write what we have done.

In theory, this approach should provide clear and documented tracking of all activities important to safety. However, it could give rise to ambiguities, gaps or inadequacies between what has been prepared, for example for component manufacture or, in operation, for maintenance work, and the reality that operators and workers must contend with. The setup technicians or engineers who write what others are going to do must have an accurate analysis of the particular risks involved in the operation in question and a good technical background to determine what must be done, but may not know the details of how to perform the operation. In contrast, such details are within the normal scope of the personnel performing the relevant operation, but they may not recognize their actual working methods in the written instructions they are given. Moreover, the personnel directly involved are not usually familiar with writing detailed reports.

A number of faults observed from 1978 onwards on 900 MWe unit components (underclad defects in reactor vessels and steam generator tubesheets, an anomaly observed on the control RCCA guide tube retaining pins), together with 'design anomalies', led the Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN) to produce a statutory text, the Order of 10 August 1984, on the quality of design, construction and operation of basic nuclear installations (referred to as the 'Quality Order') which, with the relevant application circular, gave structure to a number of quality-related measures. The measures set out in these texts were subsequently revised with new terminology in the 'INB Order', discussed in Chapter 2, which repealed the Quality Order.

#FOCUS

Conservatism and margins: several concepts used for design and safety analysis of pressurized water reactors[284]

The approaches used in design and, of course, in conducting safety analyses for pressurized water reactors aim to be conservative by taking into account any alteration of inputs so as to cover the hazards and unknowns inherent to these approaches. Practices in different fields (neutron physics, thermal-hydraulics, mechanics, etc.) reveal different elements that combine to form what is called conservatism, as defined below.

Provisions

Provisions are intended to cover, for example:

- predictable but not yet quantified changes in parameters such as weight, geometry, operating situations (pressure, temperature, associated time periods, etc.) and chemistry of the nearby fluids, within generally known ranges,
- any predictable differences between design drawings and as-built drawings,
- more generally, anything that is not yet defined precisely in the design phase and when the safety analysis is performed.

Penalties

Penalties are intended to set conservative values for data with variability that is random but within a known range. The term ‘penalty’ is mainly used in reactor physics studies and in safety analysis of the transients associated with incident and accident operating conditions.

Safety factors

Safety factors are intended to cover unknown hazards and uncertainties in the equipment sizing approach. This involves, for instance:

- the idealized representation of a structure by finite elements,
- the idealized behaviour of an insulator,
- a material idealized by a thermal diffusion function assumed to be uniform,
- etc.

[284] Text prepared with Michel Nédélec, member of the French Advisory Committee for Reactors and Advisory Committee for Nuclear Pressure Equipment.

Safety factors are defined in certain statutory texts or in certain sets of design and construction rules, such as:

- safety factors required by pressure equipment regulations (for example, see Section 8.6 concerning nuclear pressure equipment design and Chapter 27 for in-service monitoring of this equipment),
- safety factors in the design rules for snow and wind conditions, the Design and Construction Rules for Mechanical Components (RCC-M) or for Civil Works (RCC-G up to the N4 series, ETC-C[285] for EPR[286]), etc.

Safety factors must not be used to substantiate equipment resistance to higher thermal-mechanical loads than those planned initially (because of changing conditions of use or because of an under-estimation). They are factors used to cover uncertainty in the equipment modelling approach.

Margins

The term 'margin' should only be used to refer to the difference remaining between the value of a variable and a limit when the provisions, penalties and safety factors have been taken into account. A margin may be zero. If it is positive, understood and quantifiable, it may be 'used', for example, when it is difficult to substantiate the resistance of a system or component to higher loads than those initially planned. But a given margin cannot be 'used' to cover several difficulties – or only with the greatest discernment.

Table 6.2. The 19 subject matters covered by the WENRA reference levels (as published in 2014).

01	Issue A:	Safety Policy
02	Issue B:	Operating Organisation
03	Issue C:	Management System
04	Issue D:	Training and Authorization of NPP Staff (Jobs with Safety Importance)
05	Issue E:	Design Basis Envelope for Existing Reactors
06	Issue F:	Design Extension (Conditions) of Existing Reactors
07	Issue G:	Safety Classification of Structures, Systems and Components
08	Issue H:	Operational Limits and Conditions (OLCs)
09	Issue I:	Ageing Management
10	Issue J:	System for Investigation of Events and Operational Experience Feedback
11	Issue K:	Maintenance, In-Service Inspection and Functional Testing

[285] EPR Technical Code for Civil Works.

[286] Then RCC-CW for more recent projects (such as EPR New Model PWRs).

12	Issue LM:	Emergency Operating Procedures and Severe Accident Management Guidelines
13	Issue N:	Contents and Updating of Safety Analysis Report (SAR)
14	Issue O:	Probabilistic Safety Analysis (PSA)
15	Issue P:	Periodic Safety Review (PSR)
16	Issue Q:	Plant Modifications
17	Issue R:	On-site Emergency Preparedness
18	Issue S:	Protection against Internal Fires
19	Issue T:	Natural Hazards

Appendix: French Nuclear Power Reactors

The French nuclear power programme comprises several types of facility, the most recent and most numerous of which are pressurized water reactors.

The oldest facilities have been shut down definitively.

A.1. UNGG reactors

UNGG reactors are notable for their capacity to use natural uranium in metallic form as fuel, by using graphite as a moderator and magnesium as cladding material.

The fuel is loaded and unloaded while the reactor is operating.

A drawback is that, to achieve higher power, plant size has to be increased quite substantially. This contributed to the abandon of the UNGG reactor type in the late 1960s.

▶ UNGG reactors

Name	Power	Criticality	Final shutdown
Chinon A1	80	1962	1973
Chinon A2	230	1965	1985
Chinon A3	500	1966	1990
Saint-Laurent A1	500	1969	1990
Saint-Laurent A2	530	1971	1992
Bugey 1	555	1972	1994

A.2. Heavy-water reactor

France explored the option of building power reactors moderated by heavy water and cooled by carbon dioxide gas circulating in pressure tubes. Only one plant of this type was built: the Monts d’Arrée nuclear power plant on the Brennilis site in Finistère, also referred to as EL4. With a nominal power of 75 MWe, startup was in 1967 and final shutdown in 1985.

A.3. Fast-neutron reactors

Forecasting rapid growth in world uranium consumption, France developed, on its own at first and then in cooperation with Germany and Italy, the components of a fast-neutron reactor series that could be operated as a breeder – cooled by liquid sodium.

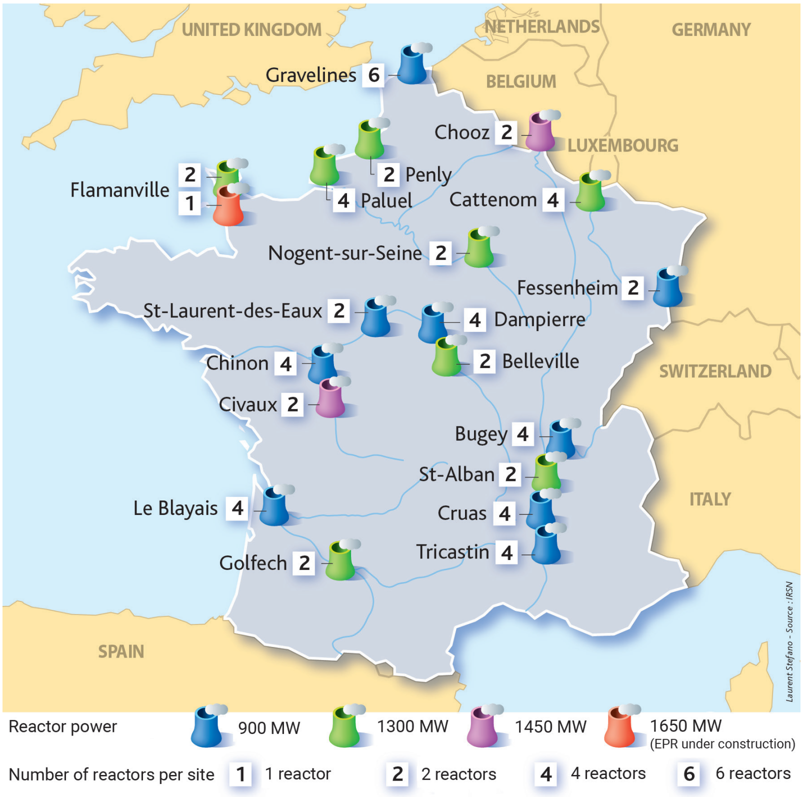
The 250 MWe PHENIX reactor achieved criticality in 1973. It was shut down definitively in 2009.

The 1200 MWe SUPERPHENIX reactor achieved criticality in 1985, but suffered various failures that affected its operation. It was shut down definitively in 1998.

A.4. Pressurized water reactors

The first pressurized water reactor unit in France, the 320 MWe Chooz A, was a Franco-Belgian project designed and built under a US licence granted by Westinghouse to the *Franco-Américaine de constructions atomiques* (Framatome) in 1959. It was started up in 1967 and shut down in 1991. Dismantling began in 2001. The reactor is located in a cave, 150 m under the ground. The design was representative of the state of knowledge in the 1960s. The experience acquired on this plant could not be used for the following units of the same type, the first of which were ordered in the early 1970s.

▶ The French PWR sites



Laurent Stefano – Source : IRSN

Grouping in standardized series

The 900 MWe plant units are twinned and share some auxiliary systems. They have a prestressed concrete containment with a leaktight metal liner. The reactor building contains the main primary system comprising the reactor vessel, three reactor coolant pumps, three steam generators and their connecting pipes.

The turbine generator unit is located ‘on a tangent’ to the reactor building for the first two series (CP0 and CP1), then perpendicular to the reactor building in later series.

The 1300 and 1450 MWe plant units are separate single units. The reactor coolant system has four loops. They have a double-walled containment without a metal liner. The annulus ventilation system, which also filters air before discharge to the atmosphere, is considered to be an engineered safety feature.

The turbine generator unit location is radial.

The lists below give the year of grid connection for each unit.

First series (called CP0) – Unit power: 900 MWe

Fessenheim 1	1977
(final shutdown in February 2020)	
Fessenheim 2	1977
(final shutdown in June 2020)	
Bugey 2	1978
Bugey 3	1978
Bugey 4	1979
Bugey 5	1979

First multiyear contract (CP1) – Unit power: 900 MWe

Tricastin 1	1980
Tricastin 2	1980
Tricastin 3	1981
Tricastin 4	1981
Gravelines 1	1980
Gravelines 2	1980
Gravelines 3	1980
Gravelines 4	1981
Gravelines 5	1984
Gravelines 6	1985
Dampierre 1	1980
Dampierre 2	1980
Dampierre 3	1981
Dampierre 4	1981
Le Blayais 1	1981

Le Blayais 2	1982
Le Blayais 3	1983
Le Blayais 4	1983

Second multiyear contract (CP2) – Unit power: 900 MWe

Saint-Laurent B1	1981
Saint-Laurent B2	1981
Chinon B1	1982
Chinon B2	1983
Chinon B3	1986
Chinon B4	1987
Cruas 1	1983
Cruas 2	1984
Cruas 3	1984
Cruas 4	1984

P4 series 1300 MWe units

Paluel 1	1984
Paluel 2	1984
Paluel 3	1985
Paluel 4	1986
Flamanville 1	1985
Flamanville 2	1986
Saint Alban 1	1985
Saint Alban 2	1986

P’4 series 1300 MWe units

Cattenom 1	1986
Cattenom 2	1987
Cattenom 3	1990
Cattenom 4	1991
Belleville 1	1987
Belleville 2	1988
Nogent 1	1987
Nogent 2	1988
Penly 1	1990
Penly 2	1992
Golfech 1	1990
Golfech 2	1993

N4 series 1450 MWe units

Chooz B1	1996
Chooz B2	1997

Civaux 1	1997
Civaux 2	1999

▶ EPR 1675 MWe unit

Flamanville 3	under testing

Video available for viewing

Defence in depth

Chapter 7
Safety Options and Considerations at the Design Phase

Obtaining the required level of safety at the the design phase of a facility such as a nuclear power reactor depends on proper application of the general objectives, concepts, principles and methods introduced in Chapter 6.

In practice, and simplifying somewhat, the primary objective in designing a nuclear power reactor is to determine all the characteristics of the 'process' (see Figure 7.1 below) that will allow electricity to be generated under the required conditions. The design process, however, is generally iterative, based initially on the choice of technical options, some of which are, of course, safety-related. These choices are supported – and corrected as needed – by verifications resulting from a certain number of studies contributing to what is known as the 'safety demonstration'.

Some technical options have an obvious link with the defence-in-depth concept covered in Chapter 6:

– the choice of the reactor site contributes to defence in depth, for example, in the choice of cooling options, the external hazards to be considered (earthquakes, flooding, human activities near the facility), the population likely to be affected by accidental release of radioactive substances, etc.;

– intrinsic neutron physics characteristics of the reactor core favourable to reactivity control also contribute to defence in depth;

- the choice of the fuel rod cladding material, which must allow the rods to withstand the various situations considered, contributes to the first four levels of defence in depth;
- neutron monitoring in the core, limitation systems (to control power, for example) and protection systems, including the reactor trip system, contribute to different levels of defence in depth;
- choices made regarding the architecture of engineered safety systems, for example, in terms of redundancy and technological diversification, are guided by the required reliability of the measures to be taken at Level 3 of defence in depth, etc.

The technical choices associated with safety considerations at the design stage – discussed in sections 7.1 and 7.2 – may thus be the result of the general objectives, concepts, principles and methods introduced in Chapter 6 and reflect historically-proven, good industrial practices. In contrast, certain systems or components may require a specific safety approach because of choices associated with major technological developments, such as computer-based instrumentation and control systems, covered in Section 7.3. The equipment safety classification concept is discussed in Section 7.4. A few points regarding the design of nuclear pressure equipment are described in Section 7.5. General considerations on provisions for hazards in facility design are discussed in Section 7.6. Certain technical choices may be associated with considerations unrelated to the primary mission of the facility: for example, the very specific risks related to nuclear facilities lead to design choices that are adopted to facilitate decommissioning, as discussed in Section 7.7.

Radiation protection for workers in operating conditions (see Chapter 31) or emergency preparedness (Chapter 38) also influence design choices for a nuclear facility.

ASN Guide No. 22 sets out general and specific recommendations on nuclear power reactor design that cover a broader scope than this chapter[287].

The study of operating conditions in the event of internal failures specific to the facility and the study of hazards are covered in later chapters. The information resulting from these studies serves two purposes:

- it contributes to the design and sizing of structures, systems and components that are important to facility safety;
- it serves for the safety demonstration, which is based on the adopted design.

[287] These recommendations are set out in parts IV to VII of ASN Guide No. 22.

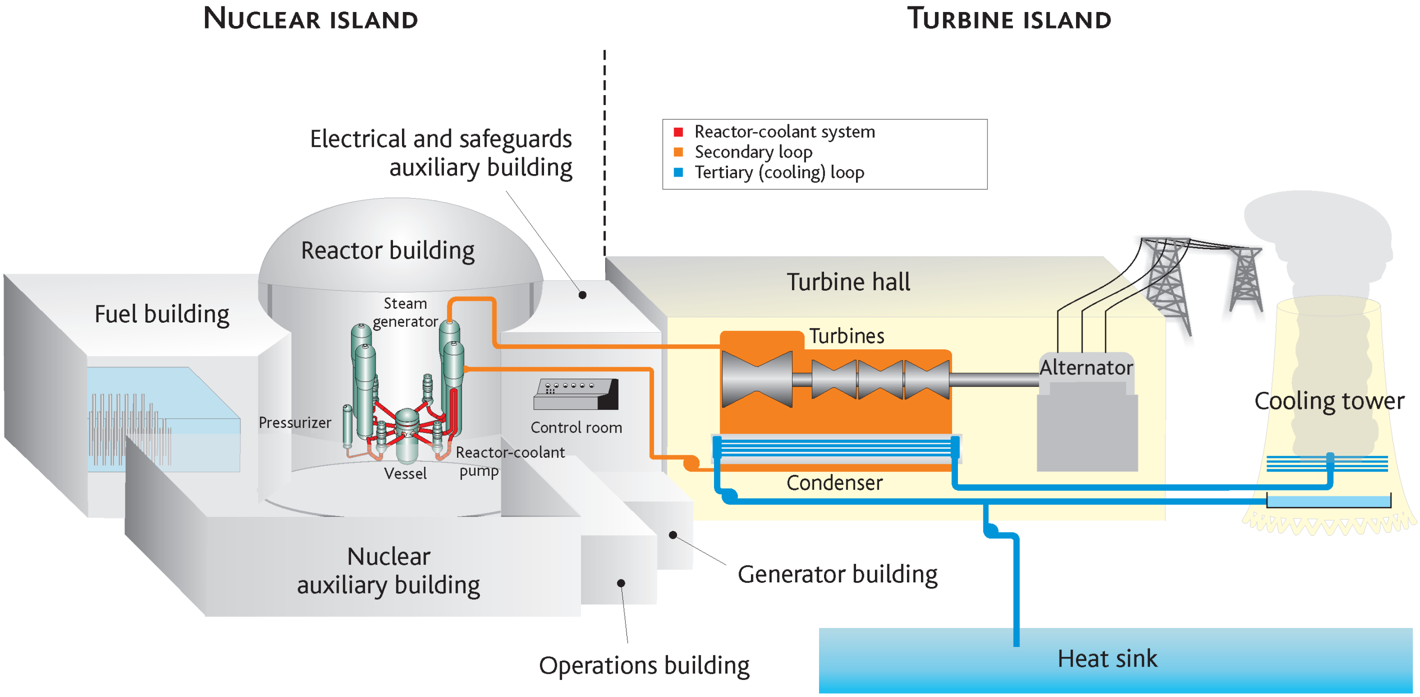


Figure 7.1. General view of a four-loop pressurized water reactor (1300 MWe or 1450 MWe) and its main systems. Georges Goué/IRSN Media Library.

7.1. Different types of design provisions associated with safety considerations

In general, designers seek to limit the potential for equipment malfunction. This relies in particular on ensuring the following points:

- the reliability of equipment and systems is sufficient to ensure that they can achieve their assigned functions or missions;
- the design is capable of tolerating deviations and the measures required to return to reference conditions;
- the design is forgiving with regard to human error.

To achieve these objectives, various types of measures are taken at the design, construction and operation stages. These measures are quite diverse and depend on whether the relevant systems and components are important to safety as provided for in the safety demonstration. Measures concerning equipment involve several aspects:

- general design, such as adopting the 'fail-safe' principle[288] whenever possible, meaning that if an equipment component fails, the equipment stays in a safe state or sets itself to a safe configuration;
- the choice of materials and sizing; for example, equipment may be designed so that its structural integrity is not compromised in various operating conditions or internal or external hazard situations;
- equipment manufacturing conditions and methods;
- equipment qualification for the different operating and ambient conditions in which it will or could be required to operate;
- procedures for inspections to be conducted during equipment manufacture and for tests carried out in the facility startup phases, then periodically during operation;
- procedures for in-service monitoring checks (periodic or otherwise), keeping in mind that it is important to design equipment that is 'inspectable' as much as possible, preferably using several methods;
- the ability to detect malfunctions using specific instrumentation, etc.

Design measures also cover systems architecture, which must display a degree of reliability consistent with a safety demonstration that meets safety objectives. An important aspect involves reducing the risk of 'common-cause failures'[289] – or 'common-mode failures' or 'common modes' – between systems or components that fulfil a similar function. For example, systems can be designed by applying measures such as:

[288] This principle is cited in the IAEA document Specific Safety Requirements No. SSR-2/1 (Rev. 1, 2016) (Requirement 26).

[289] This term is applied to dependent failures with the same direct cause (common cause) or the same indirect cause.

- dedicated emergency electrical power supplies to back up the power supply to all active components[290] in a system, ensuring system operation despite failure of the off-site power grid that provides the normal power supply to equipment;
- application of the 'single-failure criterion' to certain systems, a measure described in greater detail in Section 7.2;
- technological diversification of the components involved in fulfilling a given function, intended to limit the risks of common-mode failures (which must not be applied in principle, however, if it entails reduced reliability of the implemented technology);
- spatial or physical separation of the redundant trains to limit the risks of common-mode failures in the case of hazards (internal flooding, fire, etc.);
- appropriate design of the systems that support safety systems, to avert common-mode failures on redundant trains of the safety systems (for example, thermal conditioning systems, fluid supply systems to provide fuel [for emergency generators], electricity, compressed air, etc.).

Designers define requirements[291] that are proportional to what is required of the equipment and systems and that serve as the basis for the safety demonstration in the different operating conditions and hazard situations considered.

The measures applied must, of course, take into account human and organizational aspects. Quality control applicable to all activities involved in design, procurement, manufacture, installation, testing and inspections, and preparation for operation is of particular importance, but is only one of the many ways that human and organizational aspects are taken into consideration at the design phase, a theme covered more extensively in Chapter 16.

7.2. Single-failure criterion

Any systems that are to contribute to the prevention of incidents and accidents and their mitigation must have an appropriate level of reliability. It is difficult to conduct a detailed reliability study when the first choices regarding systems are being made. A systematic approach was implemented at the design stage, consisting of the application of a single-failure criterion for such systems[292]; this criterion can be summarized as follows: the function of a system must be fulfilled even in the event of failure of any one of its components[293].

[290] Such as pumps, valves, etc. This concept is defined in Section 7.2.

[291] Corresponding to the 'defined requirement' concept given in French regulations (since the 1984 Quality Order).

[292] Another way of improving reliability, going beyond the application of the single-failure criterion, is to introduce diversification, since using the same equipment item several times cannot significantly improve reliability, given the potential common-mode failures discussed below.

[293] Fundamental safety rule RFS I.3.a (RFS: *règle fondamentale de sûreté*).

Application of this rule is simple: it is postulated that, when the system is activated, any one of its components fails. The next step consists of identifying which component, when defective, leads to the worst consequences in the conditions under consideration.

A distinction is made, however, between 'active' components (such as pumps and valves) that require movement to fulfil their functions in the situations under study, and 'passive' components (such as tanks or vessels, pipes, heat exchangers and others).

An 'active failure' is the failure of an active component to operate when called upon[294].

A 'passive failure' is usually a leak, of limited amplitude if it can be located and stopped; if not, all the fluid escaping through the break must be considered as lost. Another passive failure could be clogging that stops the flow of a liquid.

Given the active/passive distinction, the single-failure criterion is applied as follows[295]:

- protection systems and engineered safety systems must be capable of fulfilling their function despite any active failure;
- protection systems and engineered safety systems that must operate for long periods of time must continue to operate even if a passive failure occurs after 24 h; moreover, it is necessary to ensure that a passive failure occurring before 24 h does not entail a very significant increase in the consequences of the accident (leading to a cliff-edge effect[296]).

There have been many discussions on how to apply this criterion in practice, especially with regard to two related issues:

- How should unavailability of systems or components be taken into account when they are known to be unavailable (due to a fault or maintenance) before the situation considered occurs?
- Is it necessary to take into account human error and, if so, how?

Some builders have chosen to install systems with triple or quadruple redundancy, where each train (channel or line) is capable of fulfilling all or part of the function. These are referred to as 3-train or 4-train systems. These measures may also be stipulated in regulatory requirements.

In implementing the process defined by the licensor Westinghouse, the French operator and the architect engineer studied a wide range of options for the 900 MWe plant units, then designed an architecture of engineered safety systems comprising

[294] This does not preclude the need to investigate potential inadvertent operation of active equipment.

[295] A clear distinction should be made between the design criterion defined in RFS I.3.c and the single aggravating event defined for safety studies, covered in Chapter 8.

[296] Defined in the Focus feature in Chapter 8.

two electrical trains (train A and train B) capable of fulfilling their function even in the event of a component failure. This configuration, applied up to and including the 1450 MWe plant units, limits the number of components required and consequently the amount of investment. However, it also calls for a very high level of vigilance regarding availability of the two trains. In particular, this imposes severe constraints on the maximum admissible duration of unexpected component downtime, and strict limitations on scheduled unavailability of a train, for maintenance for example, during operating periods when the relevant system is necessary for safety.

In the case of the Flamanville 3 EPR, the engineered safety features of the reactor are ensured by several physically independent trains. For example, the safety injection system (SIS) has four redundant trains, each one – connected to one of the four electrical trains – capable on its own of fulfilling the required safety function of the system. This configuration is based on a scenario in which one train is unable to inject water into the reactor because of the accident (a loss-of-coolant accident), a second train is unavailable in application of the single-failure criterion, and a third train is unavailable due to ongoing preventive maintenance[297].

Basic application of the single-failure criterion provides confidence in the capacity of the relevant systems to fulfil their assigned functions. However, to render sufficiently improbable simultaneous failures of two redundant trains (common-mode failures), a double condition must be satisfied:

- the possibility of a given hazard affecting components on both trains must be avoided;
- simultaneous failures on several identical components must be limited, as far as reasonably practicable.

The first condition entails application of very strict location and installation rules. The components of the different trains of the redundant system may be placed in different rooms, completely separated. For example, the principle of spatial separation explains why the two diesel generators of a plant unit are located in two different rooms at a distance from each other (the distance is defined so that even an aeroplane crash on the facility could not directly affect both rooms at the same time). An example of the component layout for the engineered safety systems SIS and CSS of a 1300 MWe P4 series unit is shown in Figure 7.2.

Complete spatial separation, however, is not always possible. Physical separations by screens or walls can be installed in such cases. Problems of this type arise in particular for electrical or instrumentation and control (I&C) components, for example in the control room.

It is much more difficult to identify and take into account the potential common-mode failures in the second condition. There may be design, manufacturing or maintenance errors that could impact several components simultaneously. These are faults involving the general quality of the facility or its operation.

[297] The other EPR engineered safety features are covered in Chapter 18.

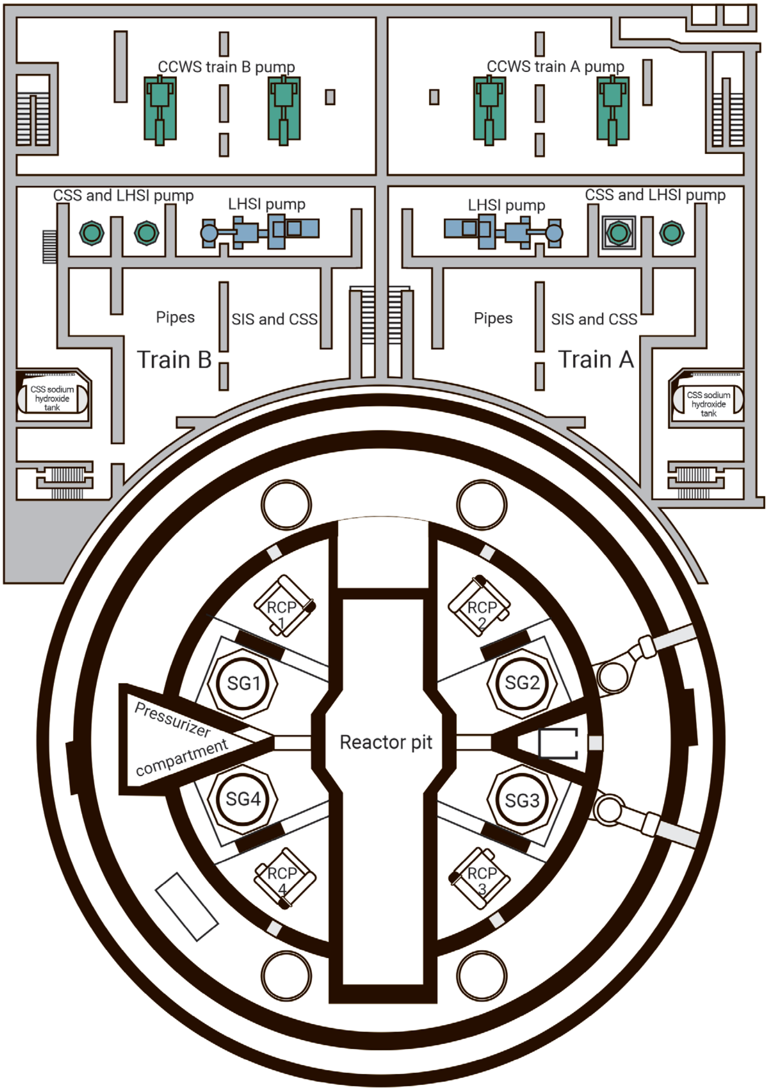


Figure 7.2. Location of SIS and CSS engineered safety system components in a 1300 MWe P4 series unit. IRSN.

It is important to note that component reliability studies show that the gain in reliability resulting from an additional instance of redundancy decreases as the number of trains increases.

Prevention of common-mode failures must also consider a factor that has only gradually been perceived as important. This concerns the influence of human and organizational factors and failures related to maintenance or control activities. The

Three Mile Island accident in the USA in 1979 raised awareness of the importance that should be given to human factors from the design stage. It took a few more years before examples of work or maintenance errors that jeopardized the availability or the satisfactory operation of some or even all of the components fulfilling a safety function were identified, declared and analysed.

The following examples are among the most significant, but are obviously not sufficient to determine the probability of common-mode failures.

The first example involves a unit at the Philippsburg nuclear power plant in Germany (Karlsruhe region). Given the redundancy levels assigned to the various systems important to safety, it had eight diesel generators. During a routine check in 1987 on a threshold setting of the diesel generators, a maintenance team that did not know the equipment well and used a somewhat ambiguous procedure left the eight generators in a state preventing their automatic startup. A round conducted 15 h later detected the error and it was corrected.

In France, several anomalies of the same type occurred in reactors in 1989, such as leaving incorrect parts in the three safety relief valves of a pressurizer, or isolating four out of the five water level sensors on another pressurizer. This subject will be covered in further detail in Section 22.2.1.

7.3. The specific nature of computer-based systems (based on instrumentation and control software)

Among the various functions fulfilled by instrumentation and control (I&C) systems, one of the most important roles is ensuring nuclear reactor safety. This importance drives the particularly sustained efforts of international working groups and standardization organizations in this field.

Instrumentation and control systems for nuclear power reactors take part in the monitoring, control, limitation and protection functions of the facility. They are generally considered to comprise three subassemblies:

- interfaces with the ‘process’, i.e. sensors and actuators that trigger actions, based on either ‘on/off’ or ‘continuous’ operation;
- programmable logic controllers (PLCs), which process measurements and operator commands, send commands to actuators, and generate the information necessary for operation;
- interfaces with operators (via control systems) and maintenance teams.

I&C systems serve to perform functions such as:

- the reactor protection functions, for example, reactor trip or activation of engineered safety features;

- functions necessary to reach a safe state[298] following an incident or accident situation;
- automatic and manual functions used in normal operation.

I&C systems are organized in an architecture intended to satisfy functional requirements (where certain systems must communicate with others) and safety requirements (when independence is necessary between certain systems).

The development of digital technologies offers increasing computation and interconnection capabilities, enabling implementation of high-performance I&C systems. For pressurized water reactors, this can include advanced functions such as computation of the departure from nucleate boiling ratio (DNBR) in the core (concept described in Section 5.6), real-time detection of component failures, or more sophisticated interfaces with operators.

This type of technology was introduced gradually, starting with the 1300 MWe reactors (P4 and P'4 series), followed by the 1450 MWe reactors (N4 series). Digital technologies raise specific issues, however, in terms of the safety demonstration, which have led the interested parties (Siemens, Framatome, Électricité de France [EDF] and IRSN) to develop a specific approach. This approach has evolved over time, taking into account technological developments such as networked communications, as well as scientific and technological progress, including formal verification methods based on mathematical approaches. It is consistent with the international consensus expressed in documents issued by the IAEA and the International Electrotechnical Commission (IEC), and is similar to approaches adopted in other industrial sectors where I&C fulfils functions important to safety, such as avionics, space or railways.

In 2000, the ASN published fundamental safety rule RFS II.4.1.a entitled *Logiciels des systèmes électriques classés de sûreté* (Software for Safety-Grade Electrical Systems), prepared at the time with IPSN and system manufacturers. It aims to "define the principles and the requirements to be met for the design, production, implementation and operation of software for computer-based systems important to safety". More recently, in January 2018, IRSN posted on its website a document in its Approaches to Safety[299] series, entitled Principles Relating to the Digital Instrumentation and Control Design Approach. This approach, directly in line with RFS II.4.1.a, gives in-depth information on the principles and requirements in the fundamental safety rule, taking into account experience acquired in assessments conducted for the French nuclear power plant fleet, in particular those relating to I&C systems specific to the EPR, benefiting from discussions with nuclear sector experts and reflecting French practice.

In certain cases, the functions associated with computer-based systems may suffer failures due to inadequate logic, consequently representing a source of system failures different from random component failures, which raises questions about their consequences.

[298] Defined in the Focus feature in Chapter 8.

[299] This is considered as IRSN's knowledge base for its expertise activities.

Although hardware failures that could potentially affect safety systems are taken into account by implementing redundant architectures along with appropriate periodic testing and preventive maintenance, faults with an impact on software are of a different nature and cannot be prevented or analysed using the same means.

The conventional approach to software development, for example, that used to develop office productivity software, does not include a sufficiently stringent design control process, resulting in products that cannot be verified, containing many faults. Moreover, attempts to control software reliability without giving priority to eliminating logic faults have proven to be inadequate. For example, running several versions in parallel and hoping to mask the faults of each version using majority voting is not very functional in practice, and experiments have demonstrated the inadequacy of this method. Probabilistic analyses to estimate failure rates are not applicable to software evaluation, and analyses of failure propagation, used successfully for equipment components, are also not applicable to software.

That is why, as indicated above, a specific approach has been adopted for the design of computer-based I&C systems for nuclear reactors, considered capable of providing appropriate substantiation of their validity. It is based on controlling the different stages of the industrial process: specification of the design requirements, design, production and integration (of the system components), each including verifications, with a final independent validation stage as an additional precaution.

The approach is supplemented by functional diversification intended to compensate a postulated design or production fault in certain functions by other functions using different physical signals or processing functions. In addition, a postulated technological failure in a family of computers is compensated by a method based on using different software and hardware mechanisms and components.

7.4. Equipment safety classification

7.4.1. Importance of equipment for safety and safety classification

Achieving and maintaining an appropriate safety level requires an approach ensuring that equipment[300] is subject to the appropriate requirements in terms of design, manufacture, qualification, operation and in-service monitoring, commensurate with its importance to safety. That is the purpose of safety classification.

[300] The term ‘equipment’ as used in this section refers to equipment items (structures and components) or systems comprising components (covered by the acronym SSC, for structures, systems and components), considered as ‘items important to safety’ as defined in the French Quality Order of 10 August 1984. ASN Guide No. 22 extends the concept of classification to ‘items important to protection’, a concept defined in the Nuclear Transparency and Security Act (*Loi relative à la transparence et à la sécurité en matière nucléaire*, or TSN Act) (see Section 2.2).

Equipment can be classified according to its role in the prevention and mitigation of incidents and accidents, its function as a means of protection against hazards, and the type of equipment in question (mechanical, electrical, etc.).

Assigning equipment to a small number of safety classes simplifies design by attributing common requirements to all the equipment in a given class.

The safety classes used by EDF are listed below for the 900 MWe, 1300 MWe and 1450 MWe reactors (the case of the Flamanville 3 EPR is discussed further below). A brief explanation of the characteristics of each class is provided, including classes referred to as 'non-safety-grade', an expression that is semantically ambiguous, but historically logical:

- mechanical pressure equipment is placed in classes 1 to 3 and the 'non-safety-grade' class;
- non-pressure mechanical equipment is classified as 'safety-related' ('LS'[301], specific to the 1300 MWe and 1450 MWe series reactors) or 'non-safety-grade';
- electrical equipment is placed in classes 1E, D (specific to 1300 MWe reactors), 2E (specific to the N4 series) or is 'non-safety-grade'.

Last in the list is the IPS-NC[302] class for equipment that is 'important to safety – non-safety-grade'. In IPS-NC, 'non-safety-grade' means that the equipment in the class was not classified at the initial design stage of existing reactors, although it is important to safety; the class IPS-NC is a safety class in its own right and has associated quality assurance and periodic testing requirements.

Civil works are also classified according to their importance to safety.

▶ Safety classes defined initially for 900 MWe and 1300 MWe reactors

When the 900 MWe and 1300 MWe reactors were first designed, only classes 1 to 3 and 1E were used by EDF. They have been updated since then, but are still in force. At that time, interest was focused on the design of protection systems and engineered safety systems, in particular on the first phases of the accidents during which these systems are activated automatically.

Class 1, with the strictest requirements, applies to pressure-retaining mechanical equipment, failure of which would result in a loss-of-coolant accident (LOCA) corresponding to a category 3 or 4 operating condition, depending on the size of the break (see chapters 8 and 9).

Class 2 applies to pressure-retaining mechanical equipment of systems conveying reactor coolant but not included in safety class 1; components of systems necessary for confinement of radioactivity in the event of a LOCA (including mechanical components of engineered safety systems, such as the safety injection and containment spray

[301] In French, *Lié à la sûreté*.

[302] In French, *Important pour la sûreté – non classé*.

systems); containment penetrations; and equipment containing radioactive fluid (such as certain components in the reactor coolant chemical and volume control system [CVCS]).

Class 3 applies to pressure-retaining mechanical equipment important to safety, but not placed in safety classes 1 or 2. It thus applies to equipment whose failure has no direct radiological consequences, and to equipment whose failure could lead to release of radioactive gases stored for decay purposes. In particular, class 3 includes the mechanical equipment in engineered safety feature support systems.

Class 1E applies to electrical equipment for:

- reactor trip,
- emergency core cooling,
- residual heat removal from the reactor,
- heat removal from the reactor building,
- containment isolation,
- prevention of significant release of radioactive substances to the environment.

Civil works are safety-grade if they:

- fulfil a safety function,
- support, protect or house safety-grade mechanical or electrical equipment,
- provide biological shielding against ionizing radiation or confinement of liquid or gaseous radioactive substances.

▶ Additional safety classes for 900 MWe, 1300 MWe and 1450 MWe reactors

As indicated above, the safety classes applied when the 900 MWe and 1300 MWe reactors were designed mainly targeted equipment whose failure could result in an accident and system components involved in the automatic reactor operation phase following an accident. Several studies have shown that this approach was too restrictive and that in practice the safety demonstration was based on a larger number of systems and components that merited a safety classification.

For example, in the event of a steam generator tube rupture accident, the phase during which the operating crew must intervene manually is essential in terms of limiting radiological consequences. The systems used for this purpose are not the safety-grade engineered safety systems classified according to the principles presented above, but rather equipment actuated manually by operators, not classified as safety-grade according to the above principles, for example the secondary system relief valves for discharge to the atmosphere, used to cool the reactor coolant system to bring it to a safe state, and the pressurizer water spray system, indispensable for reducing pressure in the reactor coolant system, thereby limiting release of radioactive substances.

Consequently, in the 1980s, the safety-grade classification for electrical equipment was extended by the introduction of class 2E for 1450 MWe reactors and class D, applied retrospectively to 1300 MWe units, for equipment used during human intervention[303] required to allow the reactor to reach and maintain a safe state following an accident situation. Similarly, the non-pressure-retaining mechanical equipment used in the safety demonstration, which had not been classified as safety-grade, was designated as 'safety-related' (LS).

Lastly, for reactors already built at that time (900 MWe and 1300 MWe series P4), the IPS-NC class (important to safety – non-safety-grade) was introduced for the mechanical and electrical equipment necessary to allow the reactor to reach and maintain a safe state as defined in the design-basis operating conditions and in the complementary conditions – see chapters 8 and 13). This class was subsequently extended to all reactor series, covering all measures necessary for protection against internal or external hazards (fire, flooding, explosion and others), and to non-essential equipment that nonetheless facilitates or improves accident operations.

▶ EPR (Flamanville 3) safety classes

Safety classification of EPR structures, systems and components reflects:

- the importance of the safety function that they fulfil, which serves to define the 'functional' classification;
- their importance as a confinement barrier, which depends on the potential release of radioactive substances, both inside and outside the facility, that could result from their failure; this criterion serves to define the 'mechanical' classification.

Defining the functional classification involves three physical states of the reactor:

- controlled state: sub-critical core, short-term heat removal ensured, for example by the steam generators, stable core-water inventory, tolerable radioactive release;
- safe shutdown state: sub-critical core, long-term residual heat removal ensured, tolerable radioactive release;
- final state: sub-critical core, residual heat removal ensured by reactor coolant system or secondary system, tolerable radioactive release.

All the safety functions (and the structures, systems and components fulfilling these functions) necessary for reaching a controlled reactor state in the PCC-2 to PCC-4 reference operating conditions (corresponding to design-basis categories 2 to 4 for the EPR) are classified F1A (designations specific to the EPR are given in sections 8.1 and 13.5).

[303] Phase C, after the 'automatic' phase B (see Section 8.4).

All safety functions required beyond the controlled state to reach and maintain the safe state in reference operating conditions PCC-2 to PCC-4 are classified F1B.

Noteworthy functions classified F2 include:

- safety functions necessary to reach and maintain the final state for RRC-A operating conditions;
- any functions necessary to prevent significant release of radioactive substances and to reach and maintain a controlled state in the event of a postulated accident with core melt (RRC-B);
- the functions designed to control internal or external hazards.

Mechanical classification involves all equipment items or portions of system lines which:

- can lead to a release of activity significantly greater than the contamination level in the surrounding environment if they fail in PCC-1 to PCC-4 and RRC operating conditions;
- or contribute to an F1A or F1B safety function.

The mechanical classes are:

- M1 for the main primary system;
- M2 for equipment items or portions of system lines that are expected to operate in situations where they are likely to convey reactor coolant when fuel cladding integrity is not ensured (safety injection, for example);
- M3 for the other safety-grade mechanical equipment items or portions of mechanical system lines (such as the engineered safety feature support systems).

7.4.2. Generic requirements associated with the different safety classes

Generic requirements are associated with the different safety classes. The differences between classes are illustrated below for the classes defined for the 900 MWe, 1300 MWe and 1450 MWe reactors. A similar approach was applied for the Flamanville 3 EPR. Qualification requirements are discussed in Section 7.4.3.

▶ Design, manufacturing and in-service monitoring requirements

Safety-grade equipment in classes 1, 2, 3, safety-related (LS), 1E, 2E and D and safety-grade civil works must comply with the following requirements:

- a design and construction code must be applied that defines computation, procurement, construction and siting methods;

– quality assurance procedures must be implemented (as required in the 2012 INB Order, applied after requirements in the 1984 Quality Order);

– periodic in-service tests must be conducted (periodic in-service monitoring for civil works structures);

– they must withstand seismic loads.

In addition, redundancy and emergency-supplied electrical power are required for class 1E and 2E electrical equipment. In contrast, redundancy and emergency-supplied electrical power were not required for the class D electrical equipment in 1300 MWe reactors, although in most cases they were implemented.

The first design and construction codes applied to safety-grade equipment were US codes (namely ASME codes), which have gradually been replaced by the following French codes:

– Design and Construction Rules for Mechanical Components[304] of PWR Nuclear Islands (RCC[305]-M), which replaced the ASME III code; the 1986 revised version of RCC-M was accepted[306] by the French safety autority in the same year. RCC-M was first used for the 1300 MWe units of the Cattenom nuclear power plant for classes 1 to 3, with a decreasing level of requirements (in particular regarding manufacturing inspections) from 1 to 3;

– Design and Construction Rules for Electrical Components of PWR Nuclear Islands (RCC-E) replacing the IEEE[307] standards for classes 1E and 2E; the 1984 revised version of RCC-E was accepted by the French safety autority, also in 1986.

A brief view of the RCC-M code is given in the Focus feature at the end of this chapter.

The civil works for the first reactor units of the French nuclear power plant fleet were built according to 'special instruction books' joining French rules and practices (Ministry of Public Works and Transport rules), and the ASME III code for metal structures. The 1981 revised version of RCC-G (design and construction rules for civil works in PWR nuclear islands) was accepted by the French safety autority. Since 2006, for the Flamanville 3 EPR (and for periodic reviews of the other French nuclear power units), the Rules for Design and Construction of PWR Nuclear Civil Works (RCC-CW[308]), incorporating Eurocodes[309], have been used.

[304] French design and construction codes use the term '*matériel*' (component) rather than '*équipement*' (equipment).

[305] In French, *Règles de conception et de construction*, RCC.

[306] Acceptance was accompanied by conditions for use of the code. This acceptance was translated into the fundamental safety rules cited in the appendix to Chapter 2.

[307] Institute of Electrical and Electronics Engineers (a professional organization).

[308] CW for Civil Works, or also ETC-C (EPR Technical Code for Civil Works).

[309] Eurocodes are European standards for sizing and substantiating building and engineering structures, available at http://eurocodes.fr/.

RCC-C, Design and Construction Rules for Fuel assemblies in PWR Nuclear Power Plants, used since the late 1980s, and RCC-I, Design and Construction Rules for Fire Protection in PWR Nuclear Islands, have been used since the early 1980s.

For the EPR, the requirements associated with electrical equipment functionally classified F1A and F1B are identical to those applied to equipment classified 1E and 2E for previous reactors. The requirements associated with mechanical pressure equipment classified M1, M2 and M3 are identical to those applied to equipment classified 1, 2 and 3, respectively, for previous reactors. It should nevertheless be noted that use of the US ASME and IEEE codes and rules defined by the German nuclear safety committee KTA are authorized under certain conditions.

▶ Functional requirements

Functional requirements depend on the safety function fulfilled by the equipment.

The only functional requirement defined for electrical equipment is to perform the function that they must fulfil (i.e. they must provide functionality).

As discussed in Section 7.2, a distinction is made for mechanical equipment between ‘active’ equipment (valves, pumps, check valves, etc.) containing mechanisms or moving parts that must complete a movement to fulfil their safety functions, and ‘passive’ equipment (vessels or tanks, pipes, heat exchangers, etc.). Three types of functional requirement are defined:

1. Integrity[310] for a pressure barrier, which applies to the pressure boundary of passive mechanical equipment, designed to ensure that the equipment confines the conveyed fluid.
2. Functional Capacity, which applies to passive equipment that conveys a fluid; the requirement limits the acceptable deformation of such equipment such that there is no reduction in the fluid flow rate that would prevent fulfilment of the relevant safety function.
3. Operability, which applies to active mechanical equipment; the requirement stipulates that mechanisms or moving parts (valves, check valves, relief valves, etc.) whose motion is necessary to fulfil the equipment safety functions must operate correctly.

Functional requirements are a factor in the choice of the rules and criteria used in mechanical component design and construction codes, to be applied when designing (sizing) the relevant components. Codes define the computation methods applicable to components (classified in levels – refer to the Focus feature at the end of this chapter) in order to ensure their resistance to various types of damage. For each level, RCC-M

[310] This term (*intégrité de la barrière de pression*) is used in French regulations. They define barrier integrity as the “absence of irreversible alteration of a barrier that could jeopardize the effectiveness required in the nuclear safety demonstration” (ASN Guide No. 22, Appendix 1). According to this definition, a leak can be considered as a loss of integrity.

defines four levels of criteria, A, B, C and D in order of decreasing stringency, that are associated with specific rules and limits (or criteria).

▶ Requirement on resistance to seismic loads

A seismic classification is defined in parallel with the safety classification. It applies to equipment that must continue to operate or maintain its integrity when subjected to loads resulting from an earthquake. For all reactor series, seismic loads have been considered at the design stage for sizing safety-grade equipment, resulting in seismic classification of class 1, 2, 3 and safety-related (LS) mechanical equipment and class 1E, 2E and D electrical equipment. The seismic classification of items that are 'important to safety – non-safety grade' (IPS-NC) is defined case by case, according to their role in situations potentially caused by an earthquake.

EPR equipment in functional classes F1A and F1B or mechanical classes M1 or M2 is seismic-grade equipment. The seismic classification of F2 and M3 components is defined case by case, according to their role in situations potentially caused by an earthquake.

Seismic-grade equipment must satisfy its functional requirements when it is subjected to the loads resulting from a seismic margin earthquake (SME) or a design-basis earthquake (DBE)[311].

7.4.3. Qualification of equipment for accident conditions

Qualification consists in demonstrating that equipment important to safety is capable of fulfilling its functions under the conditions to which it may be subjected (in terms of temperature, pressure, humidity, irradiation, seismic loads, etc.).

The equipment qualification process begins at the reactor design stage by identifying the requirements to be met by the equipment. It continues by defining and implementing a qualification programme providing appropriate substantiation that the requirements are satisfied. The objective is to complete the process, as far as possible, by the time the reactor is commissioned.

The following conditions are taken into account in the qualification process:

- degraded ambient conditions under which the equipment must operate, in terms of pressure, temperature, humidity and irradiation;
- seismic loads, for seismic-grade equipment;
- specific conditions: for example, the capacity of a valve or check valve located on a high-energy line to isolate a break in the pipe, or the capacity to convey a

[311] These concepts are defined in Section 12.3. The DBE may be an upper bound of the seismic margin earthquakes (SME) specific to reactor locations, as is the case for the French nuclear power reactor fleet. The same applies for the operating-basis earthquake (OBE) with respect to the maximum historically probable earthquake (MHPE).

radioactive fluid loaded with debris (such as equipment in systems recirculating reactor coolant from the reactor building sumps).

Qualification for accident conditions is required for electrical equipment and active mechanical equipment subject to an operability requirement. For passive mechanical equipment, it is assumed that applying the appropriate design criteria is sufficient to ensure that it meets the relevant functional requirements (integrity, functional capacity), with no additional demonstration required. However, equipment forming part of the third confinement barrier and its extension (see Section 6.3) is subject to a leaktightness requirement that may call for qualification of passive components that could be subject to degradation under the defined accident conditions (as in the case of elastomer seals).

Coatings and paints (on concrete walls, for example) inside the reactor building must also be qualified for degraded ambient conditions (pressure, temperature, humidity, etc.), in order to ensure that under accident conditions they do not produce debris likely to hamper water recirculation by the sumps, the reactor coolant system safety injection system (SIS) and the containment spray system (CSS), a topic discussed in Chapter 9.

In addition to accident conditions, qualification also takes into account equipment and coating ageing due to the effect of temperature, irradiation and mechanical loads (vibrations, etc.) throughout facility lifetime.

Up to 2006, one of the three standard qualification profiles below was applied to equipment to be qualified:

– Profile K1 for equipment located in the reactor building, necessary under accident conditions leading to degraded ambient conditions in the building. Profile K1 (see Figure 7.3 below) is bounding for the worst-case accident ambient conditions defined (other than an accident with core melt), i.e. conditions potentially resulting from a loss-of-coolant accident or a steam line break;

– Profile K2 for equipment located in the reactor building that must be capable of fulfilling its functions in normal ambient conditions;

– Profile K3 for equipment located outside the reactor building; however, equipment necessary under accident conditions leading to degraded ambient conditions in the rooms where it is located (for example, in the bunkers housing steam lines) and equipment that potentially must convey radioactive fluid loaded with debris (SIS and CSS components) also underwent qualification for these specific conditions (profile K3AD).

As of 2006, six different families of ambient conditions were defined by EDF and were taken into account to qualify equipment in the reactor building, thereby adapting equipment qualification to the radiation doses encountered in accident situations and to the time periods during which equipment operability must be ensured under degraded ambient conditions. The definition of the families of ambient conditions is based on two parameters:

- type of ambient accident conditions to which the equipment might be exposed during its operation;
- duration of the accident phase during which the equipment must be capable of fulfilling its function.

Families of ambient conditions had already been defined in the 1990s for equipment located outside the reactor building, based on the same parameters.

Taking into account families of ambient conditions made it possible to approve qualification of existing equipment for accident conditions, even when it was subject to deviations. An example is provided by the motors of the RHRS pumps, for which the accident radiation doses correspond to family 4, while the maximum dose defined for the components used in a large-break loss-of-coolant accident is that of family 6, corresponding to qualification profile K1[312].

Families of ambient conditions for the Flamanville 3 EPR were defined and applied at the design stage.

Equipment qualification can be achieved by means of tests, analyses (studies), or a combination of both.

Qualification by testing consists in subjecting 'model' equipment to loads representative of the normal and accident operating conditions that it must be able to withstand. The test programme is divided into a series of test sequences, designed to represent the load cases to which the equipment is likely to be subjected. This is the method used most often for electrical equipment.

As an example, the equipment located in the reactor building (designed to operate in the event of a large-break loss-of-coolant accident – see Chapter 9 – or a steam line break), if it is qualified by testing, undergoes the following standard test sequence (corresponding to RCC-E qualification profile K1):

- at the beginning of the qualification procedure, 'reference' tests consisting in measuring the functional and electrical characteristics of the equipment under its normal operating conditions;
- tests at the limits of the equipment operating range, aiming to characterize equipment performance under the bounding temperature, humidity and electrical interference conditions of normal operation;

[312] The family of ambient conditions for the RHRS is family 4 (degraded ambient thermal-hydraulic conditions and low-irradiation ambient conditions in the long term) because, in the safety demonstration, RHRS is taken into account only in studies on steam line break (SLB) accidents and small-break loss-of-coolant (SB LOCA) accidents. In these accidents, irradiation is low (10% cladding failure assumed for a small-break LOCA, whereas 100% cladding failure is assumed for a large-break LOCA corresponding to the profile K1 accident radiation dose). Using the dose corresponding to family 4 made it possible to reduce the qualification dose – given that the RHRS pump motors cannot be qualified at the K1 dose.

- tests to assess any possible changes in equipment performance over time, aiming to simulate equipment ageing by thermal ageing tests (case of electrical equipment), repeated-operation tests (opening/closing cycles for valves, start/stop cycles for motors, for example), vibration tests, and irradiation tests (the irradiation test may be grouped with the accident irradiation test);
- seismic resistance tests: the equipment undergoes five cycles of the accelerations corresponding to the operating-basis earthquake (OBE) and at least one cycle of those corresponding to the design-basis earthquake (DBE);
- accident irradiation tests;
- thermodynamic tests that consist in subjecting the equipment to profile K1.

The last two tests above are not conducted on equipment located in the reactor building that is qualified as K2.

Irradiation tests and thermodynamic tests are not conducted on equipment located outside the reactor building assigned to profile K3, except for equipment assigned to profile K3AD that is qualified for thermodynamic ambient conditions (such as equipment located in the bunkers housing the steam lines) or for irradiation under accident conditions (such as SIS and CSS equipment located on the water recirculation lines from the sumps).

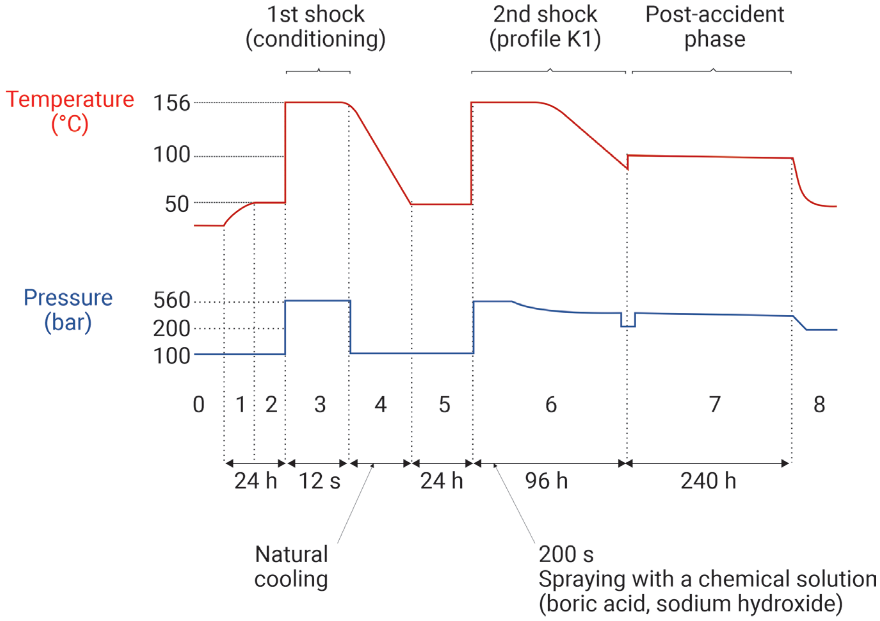


Figure 7.3. Example of qualification profile K1. Marc Bouscasse/IRSN.

Qualification by analyses can be conducted:

- by analogy, on the basis of pre-established rules (such as similar technology and dimensions), with equipment already qualified by testing, a method used in particular for valves and pumps;
- or by computation, using a simulation model representative of the relevant equipment as well as qualified computation methods or codes, a procedure used in particular for seismic qualification of valves, pumps and large equipment items;
- or by operating experience, when the corresponding conditions have been at least as severe as those that the equipment must be able to withstand.

Once the qualification of a model equipment item has been declared, it is essential to avoid the manufacture, installation, maintenance or operation of any equipment items in the facility that could compromise this qualification in the course of time. This is ensured by a series of measures referred to as 'maintaining qualification', which consists of the following:

- requiring that suppliers produce and update a reference file describing the manufacturing methods used to ensure that the components produced comply with the qualified model, and that also serves to control any engineering changes;
- once the model equipment item has been qualified, a sheet to follow up actions to maintain qualification must be prepared, specifying the applicable installation and maintenance requirements (such as the types of grease and seals compatible with qualification for ambient conditions, fastener tightening torques and locking compatible with seismic qualification); these requirements are taken into account when preparing maintenance work on the equipment. A file containing instructions for maintaining equipment qualification is used by operators to serve this purpose over time;
- controlling spare parts procurement and storage conditions.

As a general rule, equipment is qualified for a defined service life. Extension of equipment qualification may nevertheless become necessary or desirable for various reasons:

- to prolong equipment service life;
- or because the qualified service life has been revised downwards:
    - due to normal operation environmental conditions (temperature, irradiation, etc.) that are more severe than expected,
    - due to new knowledge (experience feedback, new developments) providing evidence of ageing mechanisms that develop faster than predicted or were previously unknown.

Qualification can be extended using methods referred to as Qualified Service-Life Reassessment and Extension[313]. For example, samples of reactor building electrical cables and paints have been taken for qualification testing as part of the EDF reactor operating lifetime extension project. In addition, certain components sensitive to ageing can be replaced by identical new components.

The specific qualification procedure adopted for the reactor vessel, subjected to neutron irradiation from the reactor core, is of particular interest. Test specimens of the same material as the reactor vessel are irradiated in zones close to the core and undergo mechanical testing at different times throughout facility lifetime in order to predict the mechanical behaviour of the vessel material (in particular with regard to the ductile/brittle transition threshold).

Equipment qualification for accident conditions with core melt is illustrated in Chapter 17 (for the hydrogen recombiners, the containment filtered venting system and the core catcher of the EPR).

7.5. Information on designing nuclear pressure equipment[314]

A brief outline of the history of regulations applicable to pressure equipment, and more specifically to pressure vessels used in nuclear reactors and referred to as 'nuclear pressure equipment', is given in the Focus feature in Chapter 2. Further technical details are given below on designing this type of equipment[315].

Simplifying greatly, the purpose of taking specific measures in designing pressure equipment is to ensure the safety of people, especially by averting sudden rupture of equipment during operation. In addition to technical measures taken to prevent this type of accident, safety devices (such as relief valves) are installed on the equipment to relieve pressure quickly enough to avoid any pressure rise capable of causing equipment rupture.

As discussed in Chapter 2, nuclear pressure equipment regulations[316] establish a unified and proportionate approach to the risks inherent to any type of nuclear pressure equipment, taking into account for each vessel:

- pressure and volume, which, together with the type(s) of fluid contained in the equipment item, determine the 'equipment category'; five categories

[313] The term 'progressive qualification' is also used.

[314] Information provided in collaboration with Simon Liu of ASN/DEP and Remy Catteau of ASN/DCN.

[315] Refer also to articles BN3280V1 and BN3282V1 in the magazine *Techniques de l'ingénieur*, written by Jean-Marie Grandemange (†), *Conception des enceintes sous pression* (Designing Pressure Vessels), parts 1 and 2, January 2008.

[316] The Order of 30 December 2015 on nuclear pressure equipment, the Order of 3 September 2018 amending certain measures applicable to nuclear pressure equipment and certain safety devices used for protection of this equipment.

are defined in Article R.557-9-3 of the French Environment Code, in order of increasing risk: 0, I, II, III, IV;

- the radiological inventory contained or likely to be contained in the equipment item during operation;
- whether its failure is taken into account in the reactor safety supporting documents.

Three 'requirement levels' are defined, N1, N2 and N3 (in decreasing order of stringency). Level N1 is the most stringent, applicable to "equipment items for which the safety analysis report does not define measures capable of returning the facility to a safe state, as well as nuclear pressure equipment constituting the main primary system and the main secondary system of nuclear steam supply systems...".

Level N2 covers nuclear pressure equipment items that are not classified level N1 and whose failure may entail a release of activity greater than 370 GBq, calculated as the sum of the activity of the elements present (weighted by a factor of 1/1000 for some isotopes such as tritium, nitrogen-13, and nitrogen-16).

Level N3 covers the remaining nuclear pressure equipment.

Nuclear pressure equipment regulations require that level N2 or N3 be assigned to nuclear power reactor equipment that is already in operation and belongs to safety class 2 or 3, respectively – obviously excluding the main primary system and the main secondary system, classified level N1.

Nuclear pressure equipment regulations then define a number of 'essential safety requirements'[317] for N1, N2 and N3 equipment items, which have been divided into categories I to IV – category 0 equipment, subject to lesser risks, being covered by good practice or professional guides. These essential safety requirements cover in particular:

- equipment design,
- equipment manufacture,
- technical qualification of operations required to produce and manufacture materials,
- permanent assemblies (welds, etc.) and welding operations,
- non-destructive testing to detect manufacturing faults,
- traceability of materials,
- hydrostatic tests or strength tests using a fluid other than water,
- instruction sheets specifying any particular design features that are essential to preserving equipment service life,

[317] This concept, taken from European Directive 97/23/EC, is defined in the Focus feature in Chapter 2.

- requirements applicable to materials and their mechanical characteristics.

With regard to in-service monitoring, the Order of 10 November 1999 (the Operation Order) remains applicable to the main primary system and the main secondary system of pressurized water reactors[318].

Concerning design, nuclear pressure equipment regulations stipulate that the equipment must be designed so as to minimize the risks of loss of integrity, "taking into account any foreseeable alteration of materials [...], and ageing due to irradiation". For level N1 equipment, these risks are related to:

- "low-cycle or high-cycle thermal fatigue,
- different types of thermal behaviour of materials welded together,
- vibration fatigue,
- local pressure peaks,
- creep,
- stress concentrations,
- corrosion processes,
- local damaging thermal-hydraulic phenomena,
- drainage of equipment due to a pipe break."

For each item of equipment in the nuclear power reactor fleet subject to pressure equipment regulations, the appropriate supporting documents are provided by EDF in regulatory reference files that cover materials used, manufacturing quality, protection against overpressure, 'situations' assumed for sizing (discussed further in Section 8.6), sudden break risk analysis, etc.

In the 1974 order it was explicitly stipulated that "the materials", used for nuclear pressure equipment, "must be selected so as to avoid any risk of sudden rupture in operation". For this purpose, the order defined several criteria relevant to the mechanical characteristics of materials (tensile strength, rupture elongation, impact strength). Similar criteria are specified in the nuclear pressure equipment regulations for level N1 and N2 equipment.

The installation of safety devices on equipment covered by pressure equipment regulations in order to reduce pressure and avoid rupture was discussed above. In this regard, the risks of overpressure in the main primary and secondary systems and in some of the systems connected to them, in all states of a pressurized water reactor,

[318] With a few changes introduced by the Order of 3 September 2018 (refer to the Focus feature in Chapter 2). For other nuclear pressure equipment items, appendices V and VI of the Nuclear Pressure Equipment Order are applicable.

must be reviewed in particular for the various predictable situations[319], in order to define and validate all the design and operation measures for controlling such risks. For the secondary system, it is necessary to verify that protection measures based on steam letdown lines and relief valves are adequate, while also considering reactor residual heat removal, limitation of radioactive release to the environment and prevention of excessive reactor core cooling (risk of injecting reactivity into the core).

7.6. General considerations on provisions for hazards in facility design

Certain phenomena or events may entail conditions resulting directly or indirectly in damage to equipment items in a nuclear power reactor, with consequences on safety. These phenomena or events are referred to as 'hazards'. Hazards are classified according to their origin[320] as follows:

- internal hazards when the source of the hazard is inside the facility; for example, a fire in a room, flooding following a tank rupture, the impact of a section of ruptured pipe on other equipment (a hazard caused by a phenomenon commonly referred to as 'pipe whip'), a load (such as a component during a handling procedure) being dropped on another component or system, etc.;
- external hazards of natural origin: for example, earthquakes, flooding from waterways, failure of an embankment or dam upstream of the facility, high or very high temperatures (heatwaves), strong winds, etc.;
- external hazards associated with human activity outside the facility, such as an aeroplane crash or an accidental gas explosion near the facility.

As in the case of events occurring inside the facility taken into account in the design basis, measures are taken to prevent the occurrence of internal hazards, but they are nevertheless postulated and other measures are taken to mitigate their consequences. In contrast, with regard to external hazards, other than site selection – of particular importance – design and operation measures focus on mitigation.

The availability of the nuclear power reactor equipment required to fulfil safety functions must not be compromised (as a consequence of any damage) when a hazard

[319] In the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors and in ASN Guide No. 22, the predictable situations are the plant category conditions (PCC) (see Section 6.5 and Chapter 8), and category 2 incidents combined with postulated reactor trip failure (reactor trip has a beneficial effect because it lowers the pressure in system lines).

[320] Malicious acts are also hazards, but are not covered in this book. See, for example, the document entitled A Comparative Approach to Nuclear Safety and Nuclear Security, J. Jalouneix et al., Reference Documents Series, IRSN/EDP Sciences, April 2009, and Article BN3940 V2, *Protection et contrôle des matières nucléaires* (Protection and Control of Nuclear Materials), by Jean Jalouneix, in the 10 July 2017 issue of the magazine *Techniques de l'ingénieur*.

occurs, given the associated design rules and the direct or indirect effects of the hazard (see ASN Guide No. 22), and in particular the three fundamental safety functions:

- control of reactivity (including, of course, reactor trip[321]),
- heat removal (residual heat if the reactor is shut down),
- confinement of radioactive substances.

In other words, a reactor 'safe state'[322], in which the three functions above are fulfilled without interruption, must be achievable if necessary and maintained after a hazard.

To achieve this goal, all equipment that plays a role in performing safety functions must be protected as necessary against the impact of the hazard:

- either by measures preventing the consequences of the hazard from affecting the equipment, such as safety nets to retain wind-borne debris in the event of strong winds, or protective structures capable of withstanding potential falling loads;
- or by a design that keeps the equipment in an operational state if a hazard occurs, for example the equipment designed and sized to withstand the earthquakes that serve as a reference during reactor design, or even an extreme earthquake[323].

In general, the analysis of hazard-related risks in the safety demonstration consists of two phases:

- determination of the hazard characteristics likely to affect the facility; for some hazards, a reference level is defined for facility design;
- demonstration that appropriate protection has been provided against each identified hazard.

For some hazards (such as a pipe break or internal projectiles), spatial separation of equipment important to safety can provide a way to avoid situations where the same hazard affects redundant trains. For other hazards, especially naturally occurring external hazards, specific studies are necessary in many cases, as the impact of these hazards can affect redundant trains simultaneously, or even all the systems on a site.

Other aspects of studying internal and external hazards are covered in Section 11.1.

[321] In general, a nuclear power plant operator must be able to rapidly assess the risks at hand when an external hazard occurs, in order to decide whether to maintain the reactor(s) on site in the safest shutdown state or continue facility operation (RFS I.3.b).

[322] This concept is defined in the Focus feature in Chapter 8.

[323] This concept was developed in the context of experience feedback from the Fukushima Daiichi nuclear power plant accident (see Chapter 6).

7.7. Anticipating decommissioning in the design stage

It is important for the decommissioning operations of a nuclear facility to be considered at the design stage, so that when the time comes, there are no difficulties that significantly complicate and delay the necessary operations.

In this regard, ASN Guide No. 22 on the design of pressurized water reactors includes recommendations for taking into account reactor decommissioning at the design stage: "Final shutdown, decommissioning and the targeted physical state of the facility after decommissioning must be taken into account at the design stage in order to facilitate the operations involved, while aiming to:

- complete decommissioning within the shortest possible time period;
- fully complete facility cleanup, i.e. return the site to its initial state, before structures were activated or contaminated."

It is also stated in the guide that the technical choices made at the design stage, based on experience feedback from other dismantling operations, must include:

- "equipment design and the layout of buildings and access roads. Equipment likely to contain radioactive substances in normal operation and in the event of incidents must be designed to facilitate, as much as possible, its inspection, radiological characterization, cleanup, dismantling and transport. Where pertinent, radiological shielding, easily removable for dismantling operations, must be used to reduce activation of components and equipment. Buildings must be laid out taking future decommissioning operations into account, in particular with regard to components that are difficult to handle. Any equipment likely to contain radioactive substances following accident situations must also be taken into consideration;
- materials must be selected taking into account their chemical composition and the phenomena to which they are likely to be subjected, in order to limit the risks involved in dismantling operations and facilitate the subsequent management of waste produced during these operations."

#FOCUS

The RCC-M code

The ASME design and construction code was used initially for the mechanical components (such as the reactor vessel, the pressurizer, pipes and valves) of the 900 MWe series units, 'introduced' de facto within the framework of the Westinghouse licence. Later, however, the French engineering industry developed its own equivalent code, RCC-M – Design and Construction Rules for Mechanical Components.

Like the ASME code, RCC-M defines rules reflecting best practice concerning various aspects, such as:

- selection of materials,
- type of welded assembly,
- sizing (verification of mechanical rules and criteria),
- manufacturing inspections, etc.

Three sets of rules are proposed, associated with three 'levels' of components:

- level 1 components, for which the most stringent rules are proposed,
- level 2 components,
- level 3 components, for which the least stringent rules are proposed (allowing partial manufacturing inspections, for example).

Components in safety classes 1, 2 and 3 are subject to level 1, 2 and 3 rules, respectively, although a more stringent level may be adopted on a case-by-case basis for level 2 or 3 components.

For sizing purposes (or verification of sizing), rules and criteria are devised to prevent the various anticipated damage modes for different types of loading, such as thermal-mechanical loads maintained long enough to generate a risk of creep damage, short-lived loads potentially resulting in a risk of excessive instantaneous deformation, and repeated loads generating a risk of fatigue damage.

The recommended limits – for categories A, B, C and D in decreasing order of stringency – differ not only according to the level assigned to a component – and thus its safety class – and the category of the corresponding situation considered, but also according to the associated requirement, which depends on the role played by the component. 'Non-static' components may be subjected to more drastic rules and criteria than 'static' components.

To apply rules such as those in the RCC-M code, thermal-mechanical loads and their time profiles (i.e. the design 'situations') are determined by studying postulated events in the deterministic safety analysis. These loads are usually grouped together and combined in a conservative manner (often with no claim to likelihood) before verification of compliance with the rules and criteria for mechanical components.

Chapter 8

Study of Operating Conditions in the Deterministic Safety Analysis

As stated in Chapter 6, a study of the different situations of varying severity that can affect a facility such as a nuclear reactor is an essential part of the safety demonstration for that facility.

One of the first sets of situations to be studied are situations resulting from a single initiating event that could affect one of the fundamental safety functions. This could be an equipment failure or a human error. Because there are very many situations of this kind, only a limited number, considered to be representative, are studied. In France, they have historically been referred to as ‘design-basis operating conditions’ (of the facility); in more recent texts such as ASN Guide No. 22, written jointly by the French Nuclear Safety Authority (ASN) and IRSN, they are referred to as ‘reference operating conditions’[324].

These operating conditions are defined and studied (along general lines) from the facility design phase because they contribute[325] to the development of appropriate

[324] The English expression ‘operational states’, used by the IAEA, covers both normal operation and anticipated operational occurrences or transients. Design-basis accidents also need to be included in order to cover all the ‘reference operating conditions’ as defined in ASN Guide No. 22. They all result from ‘Initiating Events’ or ‘Postulated Initiating Events’ (as defined in the IAEA glossary). Postulated initiating events (according to the IAEA) also include both internal and external hazards.

[325] Certain internal and external hazards, studied through a different approach, also contribute to facility design.

construction measures (design of structures, systems and components, including the associated protective actions).

The process of determining and studying operating conditions has been refined over time.

ASN Guide No. 22 gives definitions for a number of terms or expressions – including ‘reference operating condition’ – which are reproduced in the Focus feature below.

It is worth noting that the design-basis (or reference) operating conditions discussed in this chapter cover only some of the incidents and accidents that can affect a nuclear power reactor. The study of situations resulting from multiple failures and the study of core-melt accidents are complements to the study of operating conditions and are discussed further on in chapters 13 and 17.

#FOCUS

Terminology used in official French texts concerning events and how they are to be studied in a deterministic safety analysis

1. Designation of events

Internal hazard, external hazard

Any event or situation originating, respectively, inside or outside a basic nuclear installation that could directly or indirectly cause damage to items important for ‘protected interests’ (as defined in Article L.593-1 of the French Environment Code) or could adversely affect compliance with requirements.

(Reference) operating condition

Single initiating events are grouped together to define a limited number of reference events. A reference event is defined by the consequences of the event, such that all events leading to the same consequences belong to the same group. The incident or accident transients resulting from these events, together with normal operating conditions, constitute the ‘reference operating conditions’.

Internal failure

Malfunction, failure or damage to a component part of the facility or a component present in the facility, including occurrences resulting from inappropriate human action.

Triggering event

Internal failure or internal or external hazard likely to cause, directly or indirectly, an incident or accident situation.

Single initiating event

Internal event caused by a single internal failure.

Incident, accident

Any unforeseen event in normal or degraded operation likely to have an adverse effect on the protected interests mentioned in Article L.593-1 of the French Environment Code; the potential or real consequences of an accident are more severe than those of an incident.

2. Event analysis

Aggravating event

In a safety analysis, the worst-case single failure of an equipment item important to protection that is used for its beneficial effects when studying an incident, accident or hazard, independent of the triggering event in question. It is qualified as ‘worst-case’ with regard to the objective of the analysis.

Single failure

Failure of an equipment item to a degree that is sufficient to prevent that item from performing its expected safety function when required. Any other failures caused by this single failure of the item are considered as part of the single failure.

Cliff-edge effect

Sudden change in the behaviour of a facility caused by a slight change in the postulated accident scenario, entailing consequences that are much more severe than initially expected.

Controlled state

The state of a basic nuclear installation in which subcriticality, residual heat removal and confinement of radioactive substances are guaranteed in the short term. ‘Controlled’ means that there are no rapid adverse changes in the main parameters used to monitor the functions mentioned above.

Safe state

Stable state of a basic nuclear installation in which subcriticality, residual heat removal and confinement of radioactive substances are guaranteed in the long term. The ‘long-term’ nature of this stability is assessed in terms of:

- the facility's autonomy and the availability of external support,
- the ability to take action, if necessary,
- the values of the main parameters used to monitor the functions mentioned above and the kinetics of any changes in these values.

8.1. Categories of operating conditions

The postulated incidents and accidents taken into account in the deterministic approach, despite precautions taken to prevent them, are not all considered to have the same probability or estimated frequency, and their consequences are not assessed on the basis of the same objectives or criteria.

Generally, as mentioned earlier, a deterministic approach consists in analysing a limited number of these events, known as (design-basis or reference) operating conditions[326], grouped into categories. The events are chosen for their 'bounding' nature as regards events of the same type (or in the same 'family'[327]) in each category. The notion of 'bounding' is discussed in more detail in Section 8.2.1.

Table 8.1 lists the categories and the estimated frequency associated with each one.

Because the frequency associated with each incident or accident operating condition is an estimate based on available operating experience feedback, the figures indicated are only orders of magnitude.

Table 8.1. Categories of operating conditions

Operating Condition Categories	Order of magnitude of the annual estimated frequency of the initiating event, by reactor[328]
CATEGORY 1 Normal operating conditions	Number depends on the operations programme
CATEGORY 2 Minor but frequent incidents	Up to a few occurrences per year

[326] They are sometimes referred to as 'conventional'. This does not mean that they are unalterable; changes can be made on the basis of operating experience feedback.

[327] Events can be grouped into subsets or families according to the process functions affected: for example, variations in core reactivity related to the rod cluster control assemblies or the boron concentration in the reactor coolant system water, variations in the flow rate of the reactor coolant system water, events related to heat removal by the secondary system, etc.

[328] It is standard practice to assign a lower boundary to each category of operating conditions which corresponds to the upper boundary of the next category. In practice, only the upper boundary of each category is of interest. When the estimated frequency places an event in a given category 'N', it is not unacceptable to classify the event in a higher category (such as N + 1 or N + 2) as long as the technical acceptance criteria for category N are met.

Operating Condition Categories	Order of magnitude of the annual estimated frequency of the initiating event, by reactor[328]
CATEGORY 3 Unlikely accidents	$10^{-4} < f < 10^{-2}$
CATEGORY 4 Hypothetical accidents	$10^{-6} < f < 10^{-4}$

This table is applicable to the three types of pressurized water reactor (900 MWe, 1300 MWe and 1450 MWe reactors); the changes in terminology adopted for the EPR are explained in the Focus feature further on.

It is important to emphasize that this classification into categories is based on the estimated frequency of the single initiating event or its family. No attempt is made subsequently to assess the frequency of the actual sequence being studied, which could be claimed to have a lower frequency taking into account in particular the design rules described later on (for example, when taking into consideration an aggravating failure): the sequence cannot be separated from its design rules, and the assumed frequency of the actual sequence being studied is therefore, in principle, that of the event under consideration.

It is also important to emphasize that the frequencies chosen for internal initiating events related to equipment failures should be coherent with the measures that determine prevention of these failures: design choices (including system architecture, chosen materials and equipment design), equipment manufacturing procedures (such as assembly methods and manufacturing inspections), in-service tests and inspections, etc. Taking into account pipe breaks in the main primary system as 'hypothetical accidents' (see above table) implies that all appropriate prevention measures have been applied by the operator (see in this regard the 'prevention' section in the 'barriers' safety approach presented in Section 6.3). The 'regulatory reference files'[329] for the component parts that constitute a pressurized water reactor are obviously extremely important in this regard.

Finally, it should be pointed out that the expression 'operating condition', which covers the whole facility, should not be confused with the expression 'design-basis situation' for a system, structure or component, which will be explained in more detail in Section 8.6; however, the term 'situation' is commonly used to refer to any state of a facility.

For each category, the aim of the study on operating conditions is to make sure that certain objectives are met, which are generally translated into requirements or criteria concerning in particular the mechanical strength of confinement barriers (such as cladding) and maintaining the fundamental safety functions (such as core coolability).

[329] Regulatory reference files include the 'material' file, the 'quality of manufacture' file, the 'overpressure protection' file, the 'situations' file (see Sections 8.5 and 8.6), the 'behaviour analysis' file and the 'fast fracture' file.

As mentioned in Section 6.1, for their own intents and purposes, designers have linked the operating condition categories to targets for maximum permissible radiological consequences at the site boundary. So for the design of its first nuclear power plants and on the basis of a US standard (ANSI N.18.2), Électricité de France (EDF) proposed a table of correspondence between the range of estimated frequency of the 'design-basis' operating conditions and the orders of magnitude of the maximum consequences: for Category 1, compliance with annual site discharge permits (a few tens of μSv); for Category 2, compliance with site discharge permits per incident (a few tens of 10 μSv); for Category 3, whole-body doses below 5 mSv and equivalent doses to the thyroid below 15 mSv; for Category 4, whole-body doses below 150 mSv and equivalent doses to the thyroid below 450 mSv. The value of 5 mSv chosen by EDF for the maximum permissible consequences of Category 3 conditions was the value for annual maximum permissible exposure of members of the public as recommended in 1977 by the International Commission on Radiological Protection in its Publication 26.

EDF then made the values associated with categories 3 and 4 conditions more stringent for the design of the next series and review of the previous ones.

In any case, it should be emphasized that, in relation to the optimization (ALARA) principle developed by the ICRP, the acceptability of the measures chosen by EDF, especially during periodic reviews or new accident studies, is not assessed on the basis of 'permissible limits' or 'reference values' such as those mentioned above. In a 2013 position statement, ASN highlighted the fact that, to guide the periodic review studies associated with the fourth ten-yearly outages of the 900 MWe reactors (see Section 30.5), "EDF must introduce more proposals aimed at further reducing the radiological impact of design-basis accidents, as far as reasonably possible".

#FOCUS

Operating conditions: terminology used in the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors and in ASN Guide No. 22

The Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, applied to the EPR, use the following categories of operating conditions (Section D.1 of the guidelines):

- PCC[330] 1: normal operating conditions belonging to Category 1;
- PCC 2: reference transients, corresponding to Category 2 operating conditions;

[330] Plant Condition Category.

- PCC 3: reference incidents, corresponding to Category 3 operating conditions;
- PCC 4: reference accidents, corresponding to Category 4 operating conditions.

In addition to these PCCs, conditions involving multiple failures are also studied (explained in Chapter 13).

In ASN Guide No. 22, 'reference operating conditions' are referred to using the acronym DBC (Design-Basis Conditions).

It is important to explain exactly what the different operating condition categories cover.

Normal operating conditions (Category 1) are stable states (reactor operation at full power, at reduced power or shutdown) or transients (reactor shutdown or restart, power variation, etc.). They lie within the domain authorized by the operational limits and conditions. Any resulting discharges of radioactive substances must be completely kept under control and, of course, recorded for accountability purposes. In particular, the total annual discharges and the total for all reactors at the power plant in question must not exceed the values set by the permits for liquid and gaseous discharges at each site.

Category 2 conditions consist of minor incidents that occur at relatively high estimated frequencies. They generally take the facility out of its authorized operating domain[331]. The incidents must be controlled by control actions, mitigation actions, or even protective actions (reactor trip). By studying incidents, it is possible to confirm or alter certain characteristics of these actions (in particular, the thresholds that trigger them, for example). Any release resulting from these incidents is recorded and may lead to exceeding the levels stipulated in the discharge permits. This means that any radioactive substances released because of an incident of this kind must be discharged via controlled channels (a stack or discharge pipe), so that they are precisely known, even though they were inadvertent.

The unlikely accidents in Category 3 conditions can cause greater release of radioactive substances, but assessment of the radiological consequences for the public must show that it remains sufficiently low, even in the most adverse weather conditions.

The hypothetical accidents in Category 4 conditions are the rarest accidents to be considered in the design-basis (or reference) operating conditions. They may cause a certain amount of damage to the fuel (in terms of cladding failure or fuel melt) – which must remain limited – but it must be possible to bring the facility back to a stable situation in which cooling of the reactor core can be guaranteed in the long term.

[331] The authorized domain should not be confused with the normal operating domain. It generally allows certain deviations from the normal operating domain for limited durations and under certain conditions.

The study of accidents also makes it possible to confirm or adjust certain characteristics of protective actions (such as the reactor trip system and engineered safety features[332]).

8.2. Choice of operating conditions

To determine the design-basis or reference operating conditions, it is necessary to examine the single initiating events likely to cause:

- an inadvertent change in the nuclear chain reactions;
- excessive cooling or heating of the water in the reactor coolant system;
- a reduction in the water flow rate through the reactor coolant system;
- a loss of water inventory or water makeup in the reactor coolant system;
- an increase or decrease in the reactor coolant system pressure;
- abnormal dispersion of radionuclides: this may be, for example, the consequence of the rupture or loss of integrity on components containing radioactive substances, or damage to fuel assemblies during handling.

For spent fuel pools, the following single initiating events must be examined:

- loss of cooling in the spent fuel pool;
- reduction in the quantity of water in a pool compartment containing one or more fuel assemblies.

The initiating events of Category 2 conditions are generally found among the possible causes of variation in the parameters affecting fuel cooling (core power and therefore reactivity, water flow rate and temperature in the reactor coolant system).

Neutron flux, and subsequently the energy released from the fuel, can increase not only because of direct reactivity effects caused by:

- 'uncontrolled'[333] withdrawal of control RCCAs,
- inadvertent and gradual dilution of the boric acid in the reactor coolant,

but also because of indirect effects caused by:

- inadvertent opening of a valve in the secondary system,
- an excessive increase in power demand by the turbine.

The flow rate of the reactor coolant, which transfers the energy produced in the core to the steam generators, can be reduced by a pump shutdown, and can also be reduced more quickly if all the pumps, which are still driven by their flywheels, gradually shut down because of a loss of off-site power.

[332] Particularly loss-of-coolant accidents (Chapter 9) and reactivity-insertion accidents (Chapter 35).

[333] Term used by EDF, meaning 'inadvertent'.

Cases of malfunctioning in the steam generator main feedwater system are also studied, particularly to determine their effect on core reactivity.

A pressure drop in the reactor coolant system, which also has an adverse effect on cooling of fuel in the core, can be caused by inadvertent momentary depressurization of the reactor coolant system.

Postulated accidents, divided between categories 3 and 4, are determined on the basis of events involving equipment failures, going as far as pipe breaks, even when pipes are assumed to have been designed, manufactured and operated very conservatively, with considerable precaution.

The increases in neutron flux studied in these categories may be due, for example, to control RCCA ejection or a main steam-line break.

Water flow rate reductions in the reactor coolant system may be caused by the pumps slowing down at varying rates or even sudden seizing of a reactor coolant pump rotor.

Pressure drops in the reactor coolant system may be caused by a loss of reactor coolant through a pipe break[334], which can vary in size, up to an almost instantaneous double-ended guillotine break (known as a 2A break, where ‘A’ refers to the area in which the fluid flows through the pipe).

The assumptions associated with breaks in reactor coolant pipes are discussed in Chapter 9.

Release of radioactive gases or contaminated water from rooms where the corresponding tanks are located is also examined. The same applies to failure of the rods in a fuel assembly during handling in the reactor building or the fuel building.

This can lead to a very large number of possible events, from which a selection is made:

- by determining which cases are sufficiently representative and ‘bounding’;
- by examining the appropriateness of excluding some on the basis of a high level of prevention.

8.2.1. Concept of ‘bounding’ incident or accident

As mentioned above, the number of incidents and accidents to be studied is reduced by determining which one, within the same family, seems likely to have the most significant consequences.

For a given type of incident or accident, it may be that several types of consequences have to be taken into account, which means that several variants of the

[334] In safety language, the term ‘break’ is often used to refer to (through-wall and open) cracks in pipe walls, going as far as pipe rupture.

incident or accident are ultimately chosen and studied, which are all 'bounding' in nature but for different types of effects (or 'anticipated phenomena'), for example:

- effect in terms of reactivity insertion in the core;
- effect in terms of undercooling of the core;
- thermal-mechanical effects on the fuel assemblies and cladding, on the reactor coolant pressure boundary, on the containment, etc.;
- effect in terms of radiological impact, etc.

8.2.2. Accident exclusion

There are accident situations that could theoretically occur, but because the prevention measures appear to be sufficient, it is not considered necessary to study their consequences (which, in some cases, may not be mitigated by demonstrable industrial measures). This is the case for fast fracture of large pressure equipment items such as the reactor vessel, the outer shell of a steam generator, the pressurizer or the reactor coolant pump casings. The INSAG-10 report does not ignore these cases and recommends, as already mentioned in Section 6.4.1, that for these cases, "several levels of precautions [be] introduced into the design and operation. Such precautions may be taken, for instance, in the selection of materials, in periodic inspection [...] or in design by incorporating additional margins of safety."

Based on global industrial experience, it seems that, for some equipment, provided that it is well designed, well constructed and properly monitored throughout all stages of its lifetime, the possibility of failure can be ruled out. This is why these fast-fracture accidents are not chosen as initiating events with regard to operating conditions.

Initiators of this kind are therefore not chosen for accident studies (they are 'excluded'), provided that particularly stringent requirements are met in terms of their design, manufacture, construction and operation. It will be seen in Chapter 18 on the new-generation EPR that failure exclusions were proposed by EDF for the main pipes in the reactor coolant system and in the secondary system and were accepted by ASN, the French Nuclear Safety Authority. ASN Guide No. 22 emphasizes that failure exclusion assumptions and their conditions of application must be examined (in cooperation with safety organizations) early in the design stage.

ASN Guide No. 22 states that the use of a failure exclusion assumption "must be based on particularly stringent conditions in terms of design, manufacture and in-service monitoring aimed at preventing failure. These conditions concern:

- analysis of pertinent damage mechanisms, the choice and use of materials with sufficient resistance to these damage mechanisms, determination of the stresses that they are subject to, including when a hazardous event occurs, and verification of compliance with criteria that aim to prevent the risks of failure;

- the use of manufacturing and inspection processes which demonstrate that a very high quality level has been achieved taking into account [...] the state of the art and best practice at the time of design and manufacture, as well as technical and economic considerations compatible with a high degree of protection of health and safety;
- in-service monitoring, in particular to check in due time that the component has not suffered any damage.

In this perspective, a bounding calculation of applied stresses, analysis of the behaviour of the structures subject to these stresses, the existence of margins, especially for mechanical criteria, qualification of the manufacturing processes and renewed procurement, the choice, scope and accuracy of inspection techniques in view of the manufacturing processes to be used, the establishment of acceptance criteria for manufacturing defects, the accessibility of the areas to be monitored during operation and the scope of the associated inspections, and taking into account experience with the behaviour of similar materials or facilities, are all necessary for the implementation of this approach."

Moreover, in the 1990s, during Franco-German discussions on the safety of the next generation of pressurized water reactors (i.e. the EPR), the concept of 'practical elimination' was introduced, to be applied to certain, at least theoretically conceivable, core-melt situations potentially leading to 'significant early' releases, for which it did not appear to be possible to implement realistic measures to reduce the consequences significantly and demonstrably. This subject is discussed further in Section 17.10.2 in the chapter on core-melt accidents.

8.3. List and breakdown of operating conditions

In 1970, in the preliminary safety analysis report on the first unit at the Fessenheim nuclear power plant, which was the first 900 MWe unit built in France, the events studied were divided into three groups:

- transients and operating incidents,
- accidents requiring the use of engineered safety features,
- loss-of-coolant accidents (LOCA).

This list and its organization came from US practices and were the outcome of discussions between designers or operators and safety organizations in the USA.

The list was changed slightly to adjust to the context in France. Transients and operating incidents were placed in Category 2; accidents were distributed between categories 3 and 4, without isolating loss-of-coolant accidents in a separate category. By the mid-1970s the lists were organized as described below.

CATEGORY 2: incidents of medium frequency, the consequences of which must remain extremely limited

Reactivity

- inadvertent control RCCA bank withdrawal, reactor subcritical or at full power
- gradual uncontrolled boric acid dilution
- startup of an inactive loop in the reactor coolant system
- malfunction of the main feedwater system supplying the steam generators
- excessive increase in the turbine load

Irregularities in core physics

- incorrect position or drop of an RCCA or an RCCA bank
- partial loss of coolant flow
- total loss of load, turbine trip
- loss of off-site power, leading to shutdown of the reactor coolant pumps
- loss of normal feedwater flow to steam generators

Primary breaks

- inadvertent short-term opening of a pressurizer valve, momentary depressurization of the reactor coolant system

Secondary breaks

- inadvertent opening of a valve in the secondary system

Reactor vessel embrittlement

- inadvertent startup of the safety injection system or emergency boration system

CATEGORY 3: very infrequent accidents, the consequences of which must remain sufficiently limited

Reactivity

- control RCCA withdrawal at full power

Irregularities in core physics

- forced decrease of reactor coolant flow
- incorrect location of a fuel assembly in the core

Primary breaks

- small-break loss-of-coolant accident
- inadvertent opening of a pressurizer valve with long-term depressurization

Secondary breaks

- small-break in a steam line

Loss of confinement, radioactive release

- rupture of the chemical and volume control system tank
- rupture of a storage tank in the gaseous waste processing system

CATEGORY 4: significant hypothetical accidents, the consequences of which must remain acceptable

Reactivity

- control RCCA ejection

Irregularities in core physics

- reactor coolant pump rotor seized

Primary breaks

- loss-of-coolant accident (LOCA)
- complete rupture of a steam generator tube

Secondary breaks

- large break of a secondary system (water or steam) pipe

Radioactive release

- fuel assembly handling accident

Global experience subsequently led to the classification of a steam generator tube rupture as a Category 3 condition due to its frequency, instead of Category 4, starting from the N4 reactor series (this type of accident is discussed in Chapter 10). This change was introduced in the list of operating conditions used to design the standard 1450 MWe (N4) series, then for the EPR design. The rupture of two steam generator tubes was placed in Category 4 for the N4 series and the EPR (PCC 4).

For the 900 MWe and 1300 MWe reactors, a steam generator tube rupture was later included, for the safety reassessment studies, in both categories 3 and 4, the latter case also taking into consideration a failure that could result from the tube rupture (see Chapter 10).

These modifications led to more stringent requirements for steam generator tube rupture accidents and changes to equipment and operating procedures in order to meet these requirements[335].

Experience also showed that reactor coolant pump rotor seizure occurred at a higher frequency worldwide than originally estimated. This led to increased inspection of reactor coolant pump shafts; because of this, it was not considered necessary to modify the category of reactor coolant pump rotor seizure accidents.

The list of reference transients, incidents and accidents (plant condition categories, see the Focus feature in this chapter) in the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors is reproduced at the end of this chapter.

Note that the same type of accident or the same accident family may appear in several operating condition categories. The fact that a large break has acceptable consequences in Category 4 does not mean that a small break has acceptable consequences in Category 3, since the fuel-resistance criteria are not the same (this will be explained in greater detail later in Section 8.4.7).

8.4. Methods for studying operating conditions

As seen earlier, the operating conditions chosen are the result of a search for conceivable changes in the safety functions that can adversely affect safety. They are studied ultimately with the aim of providing protection from different types of transients or phenomena that present risks. Initiating events are studied within a range of assumptions and study conditions chosen so as to aggravate the consequences and thereby make the result 'bounding' as regards the anticipated phenomena (for a 'deterministic' demonstration).

For pressurized water reactors, incident or accident transients (operating condition categories 2 to 4) are generally broken down into three successive phases:

[335] For design of the N4 reactor series, the operator also set lower limits on radiological consequences than those adopted for earlier series.

– phase A: occurs between the initial instant of the transient and the first intervention by an automatic protection system (for example dropping RCCAs following a reactor trip) or the first manual action to be taken by operators as specified in an alarm sheet;

– phase B: takes place between the instant of the first intervention by a protection system and the instant of the first manual action;

– phase C: occurs between the instant of the first manual action and the achievement of a safe shutdown state.

The systems actuated in these different phases may belong to different safety classes (see Section 7.4).

The next part of this chapter discusses the choice of initial conditions and the conservative assumptions adopted, the 'single aggravating event' rule, the conventional combination rules, the qualification of computing resources and the criteria to be met depending on the accident category.

In official French texts[336], two concepts are used for the design and safety analysis of pressurized water reactors: the 'controlled state' and the 'safe state', defined in the first Focus feature in this chapter. The texts indicate in particular that, under reference operating conditions, a controlled state represents a stable or even an increasing water inventory in the reactor coolant system[337].

8.4.1. Choice of initial conditions, conservatism

A nuclear facility can be in various operating states, from full power to shutdown for refuelling or maintenance.

In each of these states, the characteristic parameters – pressure and temperature of water in system lines, water flow rates, voltage and frequency of power supplies, radioactivity, contamination, etc. – can vary within different ranges and the means of measuring, monitoring and controlling these parameters are not perfectly accurate.

The 'standard states' and 'operating domains' authorized by the operational limits and conditions are explained in Section 20.2.1.1 in the chapter on general operating rules. Distinct substates may be defined to study operating conditions.

During the 1980s, operating experience revealed the importance of carefully examining the risks inherent to the shutdown states of a pressurized water reactor (namely the possibility of an inadvertent decrease in water level during the shutdown state when the core is in the reactor vessel)[338]. Both the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors (applied to the EPR) and ASN Guide No. 22 highlight the importance of

[336] The following comes from ASN Guide No. 22.

[337] More details on these two concepts applied to the spent fuel pool are given in Chapter 15.

[338] This subject is discussed in further detail in Section 22.1.

studying the initiating events in the different shutdown states of a reactor. The guide emphasizes that "special attention should be given to shutdown states presenting specific conditions, particularly when certain items important to protection or certain confinement barriers are unavailable (as when the main primary system is opened, or the airlock or the equipment hatch in the containment is opened) or when workers may be present inside the containment."[339]

For each study of an initiating event, the initial conditions (associated with the initial state of the reactor) and the values of certain parameters are chosen conservatively (for example, by imposing the 'penalties' mentioned in Chapter 6) with regard to the anticipated phenomena. Accuracy of the measurement, monitoring and control systems is taken into account; the same applies to the systems used to trigger a reactor trip and engineered safety systems. The set of values may vary in the study of the different phases (see above) of the transient associated with the initiating event under study.

If the anticipated phenomenon is a 'departure from nucleate boiling' in the core, which severely degrades cooling of the cladding on the affected fuel rods and can cause them to be damaged, the values for power and average water temperature in the reactor coolant system are increased (initially and during the transient). Coolant pressure, however, is chosen by combining the conditions that reduce it.

Reactivity injection accidents due to control RCCA movement are studied based on the assumption that they occur at the start of the cycle when the neutron feedback provided by the moderator (the reactor coolant system water) is at its lowest. Cooling accidents originating in the secondary part of the nuclear steam supply system (for example, from a steam-line break) are studied at the end of the cycle when, in the absence of boron in the coolant, the effect on reactivity is at its greatest.

Moreover, if fission products normally contained by the cladding are released, the quantity of radioactive substances released is raised by assuming that the fuel is at the end of the equilibrium core cycle.

8.4.2. Consideration of an aggravating event in the study on operating conditions – 'Passive' failures

In studies on design-basis (or reference) operating conditions, an 'aggravating event' is taken into account: this is a single failure, independent of the postulated initiating event, which is applied to equipment used for its beneficial effects on the operating condition under study. The most pessimistic aggravating event must be used for each criterion to be met and for each phase of the transient. Application of the single aggravating event does not change the category of the operating state in question.

[339] ASN Guide No. 22 also explains that, where appropriate justification is provided, implausible combinations of accidents and initial states may be disregarded (i.e. special mitigation measures do not have to be planned and implemented).

The aggravating event is assumed to occur when the relevant equipment item is in use[340].

In particular:

- jamming of the control RCCA displaying the highest negative reactivity following reactor trip must be considered a possible aggravating event for all operating conditions;
- a closing failure on a main steam relief valve must be considered a possible aggravating event for operating conditions in Category 2, such as homogeneous dilution or inadvertent withdrawal of a control RCCA.

Certain failures, such as failure of the SIS accumulator valves to open, can be excluded from application of the single aggravating event rule provided that appropriate substantiation is given (assuming this information is reliable and supported by operating experience feedback).

Preventive maintenance on systems likely to be used in an incident or accident must also be taken into account. Methods have been defined for taking these systems into account in terms of unavailability of the corresponding equipment components.

Furthermore, where necessary, a 'passive' single failure should be considered in the study on operating conditions. This is a failure that occurs on an equipment item that does not need to change state to perform its function. A passive failure may be:

- a leak from the pressure boundary of a system line containing fluid; if this type of leak is not detected and isolated, it is assumed that it will grow until the flow is equivalent to a total rupture;
- another mechanical failure adversely affecting the flow line corresponding to the normal operation of a system line containing fluid.

Passive failures are taken into account for long-term operation (after more than 24 h) of engineered safety features, at a leak rate conventionally assumed to be 200 litres per minute until the leak has been isolated.

For the EPR, however, it was stipulated[341] in the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors that "sensitivity studies must be conducted to show that the case of a passive single failure in the short term (before 24 h) as well as the case of a leak rate greater than 200 L/min (up to rupture of a connected pipe with an inside diameter of 50 mm) are covered by taking into account single failures on active components or do not lead to cliff-edge effects with regard to system performance and radiological consequences."

[340] In EDF's studies, it is postulated that the failure occurs on first use. Nonetheless, it is necessary to confirm, for example in the case of a valve that opens on this first use and that should then close again, that closure cannot be prevented by this first use or by the existing conditions (fluid escaping in the form of water or steam, etc.).

[341] This is expressed in a similar way in ASN Guide No. 22.

8.4.3. Conventional combinations

The single-aggravating-event rule is not the only convention adopted in studies on design-basis (or reference) operating conditions to ensure that the conclusions are as bounding as possible.

For all Category 4 conditions, incorporating a loss of off-site power (LOOP) is considered if it has a conservative effect on the transient in question. This rule is a convention but comes historically from the combination of the mechanical effects of a major earthquake (seismic margin earthquake [SME] or design-basis earthquake [DBE] – see Sections 8.5 and 12.3) with the large breaks in Category 4, since an earthquake can lead to the loss (failure) of electrical power transmission lines that are not designed to withstand an earthquake, even of moderate intensity. A LOOP is added to the analysis at the most penalizing moment, which is generally one of the following three instants: the initial instant, the instant of reactor trip, or the instant when an engineered safety feature (such as the safety injection system) starts up. Among other consequences, a LOOP causes the reactor coolant pumps to stop.

It was seen in the previous chapter that the single-failure criterion requires all the equipment necessary to control accident situations to be at least doubled, by implementing two completely separate trains. The conventional combination of Category 4 conditions with LOOP therefore requires the electrical equipment in each of these trains to be backed up by a standalone generator that starts up automatically, independently of the off-site power supply and is fully effective in an earthquake situation.

The 900 MWe, 1300 MWe and 1450 MWe reactors are thus each equipped[342] with two diesel generators rated at several megawatts each, capable of supplying the necessary power capacity several tens of seconds after receiving a startup command, and qualified for earthquakes.

This time lapse should obviously be considered in the accident studies (since the engineered safety systems used will only reach full efficiency after a certain time delay).

Furthermore, in the initial design studies of the 900 MWe and 1300 MWe reactors, the possibility of an earthquake causing an operating incident or accident, regardless of the operating condition category (2, 3 or 4), was not considered because earthquakes were taken into account (as a ‘load case’) in the design of safety-grade mechanical and electrical equipment. However, during discussions on the N4 reactor series, IPSN considered that an earthquake could still cause an internal failure even if the equipment that failed had been designed to withstand earthquakes. Following this reasoning, which considers the earthquake as an ‘event’, it is also assumed that de ‘event-initiating’ earthquake would cause a loss of off-site power for the same reasons

[342] For the EPR, see Section 18.2.4.

as given above. For the N4 series, category 2 and 3 conditions combined with LOOP were therefore studied in light of the criteria associated with Category 4.

In studies on these combinations, the time taken for the neutron-aborbing rods to drop is extended beyond the maximum value stipulated in the operational limits and conditions (taking into account the earthquake) and only the equipment capable of performing its function after an earthquake can be used.

Since the introduction of this approach for the N4 series, verification studies[343] have been launched by EDF for the 900 MWe[344] and 1300 MWe units, for category 2 and 3 conditions, combining the LOOP (induced by an earthquake) with the initiating event, in order to verify compliance with Category 4 criteria.

The approach introduced for the N4 series was also used for the Flamanville 3 EPR.

8.4.4. Preventing accident aggravation

One of the acceptability criteria for the consequences of the incidents and accidents in categories 2 and 3 is that they must not cause an accident in the next category.

The detailed study of each of these incidents or accidents must therefore reveal any thermal-mechanical or other constraints that could impact systems, structures or components that may not have caused the initiating event, but could be led to failure subsequent to the event. A whole series of 'design-basis situations' or 'load cases' is derived from this reasoning, which must be taken into account in the design of these systems, structures and components.

The rupture of a main pipe in the reactor coolant system in one place should not cause another rupture in the same loop, nor a rupture in another loop, nor seriously compromise the safety injection system. The forces produced by deformation of a broken pipe and the jets of fluid on the concrete and on the structures of the reactor coolant pump bunkers are therefore studied in detail because they serve as a basis for designing the support structures of the affected loop and adjacent loops.

8.4.5. Operator response time

When studying the design-basis (or reference) operating conditions, operator response times are chosen that are considered to be the shortest time in which the operators can respond; these time intervals, which depend on the response location, are given in Table 8.2 below.

[343] Or 'robustness' studies, according to the terminology used by EDF.

[344] As part of the safety reassessments associated with their fourth ten-yearly outage.

Table 8.2. Chosen operator response times.

	900, 1300 and 1450 MWe reactors	EPR
Response in the control room	20 min	30 min
Response in the electrical building	25 min	60 min
Response in other buildings	35 min	

Considering longer operator response times has a beneficial impact on safety[345].

8.4.6. Using qualified simulation software

Despite the development of knowledge, it is often difficult to produce an accurate representation of the complex phenomena that can occur during an incident or accident. Designers must therefore advance cautiously when using computer simulations.

To study incidents and accidents and assess their consequences, designers[346] use either simulation software that has been recognized for its conservatism[347] in a particular field in the course of its 'qualification', which may include validation based on experimentation, or best-estimate simulation software, which reproduces experiments as realistically as possible. When best-estimate simulation software is used, multiplier coefficients may be applied to the results before they are compared with technical acceptance criteria.

Simulation software is improved continuously based on research and development work, which may make it possible to reduce the weight of conservatism through better knowledge of the phenomena at work and the means used to model them.

These improvements can also reveal that certain results produced in the past were not conservative enough. This was the case in the early 1980s for calculation of the pressure resulting from a main steam-line break within the containment of the P'4 reactor series. The available margins nevertheless allowed EDF to show that the technical criteria for containment design had not been exceeded. This example – and there are others – confirms, if necessary, the importance of high-quality studies and the need to maintain a cautious approach in the different phases in which the characteristics of systems, structures and components are defined.

To prepare emergency operating procedures, the studies conducted to check that the consequences of these events are acceptable may not be suitable for defining the actions to be taken by operators; therefore, the results of best-estimate calculations are used.

A certain number of simulation codes are presented in Chapter 40.

[345] 'Robustness' studies of all the design-basis operating conditions are carried out by EDF as part of the safety reassessment associated with the fourth ten-yearly outages of 900 MWe units, using the operator response times chosen for the EPR safety analyses.

[346] Or IRSN as part of its technical support to ASN (see Chapter 40).

[347] The term 'pessimism' is also used.

8.4.7. Main criteria to be met for fuel in the reactor core

Acceptability of the calculated consequences of plant operating conditions is assessed according to a certain number of requirements and criteria, known as technical acceptance criteria, particularly with regard to confinement barriers.

In particular, the higher the estimated frequency of the operating condition under study, the more fuel damage must remain limited.

But the reactor coolant pressure boundary, the containment and other structures, systems and components important to safety are also subject to requirements regarding different operating conditions or hazards to be taken into consideration in the design phase. These requirements are considered to be satisfied if a set of criteria are met (such as design and construction code criteria). It should be emphasized that when designing engineered safety systems, the most stringent criteria[348] in the design and construction codes are used, while assuming that accident operating conditions are the normal operating conditions for these systems: this is the case for the safety injection system, which aims to mitigate the risks of reactor coolant system breaks.

Conservatism, particularly in simulation calculations for incident or accident transients and their consequences, was discussed earlier in this chapter. Technical acceptance criteria generally take into account the uncertainties associated with the state of knowledge on which these criteria are based. When assessing whether or not the anticipated phenomena are sufficiently under control, the impact of conservatism must be clearly identified.

The next part of this chapter discusses only criteria related to fuel in the reactor core. These criteria aim to avoid cladding failures, to maintain a coolable core geometry and to mitigate the calculated radiological consequences of plant operating conditions.

Generally, for each operating condition, a qualitative objective is chosen to express the level of damage considered acceptable for the fuel. It is translated into requirements based on the physical phenomena likely to lead to this damage. Compliance with these requirements is then guaranteed by checking criteria known as technical assessment criteria, which are the calculable parameters that best represent the anticipated physical phenomena.

Three physical phenomena are likely to lead to a loss of fuel rod integrity ('cladding failure'):

- departure from nucleate boiling (sudden degradation of fuel rod cooling when a continuous blanket of steam forms on the surface of the fuel rods), which can lead to an excessive increase in temperature;
- partial or complete melting of fuel pellets or cladding;
- pellet-cladding interaction (PCI), either amplified ('assisted') by stress corrosion cracking (PCI-SCC), or purely mechanical (PCMI); this interaction occurs when

[348] Those for normal operating conditions.

fuel pellet expansion is greater than cladding expansion[349] in the event of a transient power increase.

In view of these phenomena, quantitative criteria are defined (heat flux at the cladding wall must be lower than the flux level that leads to departure from nucleate boiling [DNBR[350]], pellet melting temperature must not exceeded, compliance with a mechanical limit must be observed to ensure there is no cladding failure due to pellet-cladding interaction, etc.), which can be used to assess potential fuel rod damage. These criteria may depend on rod properties, especially the cladding material.

As will be shown later, loss of fuel rod integrity is tolerated for some operating conditions, provided that the core remains coolable. Core cooling capacity requires preserving the overall core geometry and ensuring that a sufficient amount of water circulates in the fuel assemblies. Swelling (or 'ballooning') of rods (in the event of a loss-of-coolant accident, for example) leading to excessive restriction of the passages allowing fluid to flow between the rods, or a thermodynamic interaction between hot fuel particles ejected from ruptured rods causing a steam explosion, are phenomena likely to have an adverse effect on core cooling; the array of criteria chosen takes into account these risks.

It is considered that Category 2 conditions must not adversely affect fuel rod integrity. The protection system and the operational limits and conditions of the reactor must be defined for this purpose.

However, it is acceptable for Category 3 conditions to cause limited damage to the fuel in the reactor core; fuel pellet melting at the core hot-spot must be limited – it must be avoided in the case of the EPR and new reactor projects (see ASN Guide No. 22). As indicated above, damage affecting the core must not adversely affect core cooling; one criterion concerns the cladding temperature, which must stay below a value designed to prevent the failure of fuel rods embrittled by excessive oxidation at high temperature. To ultimately limit the radiological consequences, designers set a criterion requiring that the number of fuel rods entering departure from nucleate boiling remain less than 5% of the rods in the core.

Finally, core cooling must not be adversely affected in the case of Category 4 conditions either; fuel pellet melt at the core hot-spot must remain limited. Designers have set a criterion requiring that the number of fuel rods entering departure from nucleate boiling remain less than 10% of the rods in the core. Special criteria are defined for loss-of-coolant accidents (see Chapter 9), and also for control RCCA ejection accidents (see Chapter 35).

[349] The pellet applies hoop tensile stress to the cladding during transient power increases. It is also important to note that extended operation at partial power can place additional stress on the cladding during a subsequent transient power increase because of less favourable 'conditioning' before the transient.

[350] Departure from Nucleate Boiling Ratio.

Generally, the need to meet the technical acceptance criteria associated with fuel incites designers to set[351] requirements for the design of reactor protection systems and engineered safety features, as well as operating limits for the reactor, which are then translated into operational limits and conditions; for example, for a loss-of-coolant accident (LOCA), the maximum linear power density in the reactor core is limited (referred to as the 'LOCA limit') and for control RCCA ejection, a limit is placed on the insertion depth of the rod cluster control assemblies in the core.

8.5. Concept of 'design-basis situations' for equipment

Operating conditions involve all or part of the facility and must be distinguished from the 'situations' used in the design phase for equipment design (the expression used is 'design-basis (or reference) situations'). Design-basis situations are the result of studies, and particularly computer simulations of pressure, temperature, flow rate, stress and other transients associated not only with the design-basis (or reference) operating conditions, but also with events within the 'complementary domain' ('beyond-design-basis events') and internal and external hazards (for some of these design-basis situations, the expression 'load case' is also used).

Design-basis (or reference) situations result from the study of operating conditions, which are classified into four categories; consequently, design-basis situations are also divided into four categories. All of these situations are used in what was conventionally referred to as the 'basic design'[352], now referred to as the 'design reference domain' (see ASN Guide No. 22).

Pressure equipment regulations – which, in the case of pressurized water reactors, focus particularly on the main primary system (MPS) and main secondary system (MSS)[353] – refer to a slightly different 'situation' concept that will be explained in the next section.

Moreover, conventional combinations of situations are used involving mainly two external events:

- loss of off-site power (LOOP),
- earthquake, represented by the seismic margin earthquake (SME) – or the design-basis earthquake (DBE[354]) – as well as the maximum historically probable earthquake (MHPE) – or the operating-basis earthquake (OBE) –,

themselves combined together; as stated earlier, it seems logical to combine a major earthquake with failure of electrical power transmission lines that have not been designed to withstand these earthquake conditions.

[351] In an iterative design and safety demonstration process.

[352] See, for example, the book *Démarche sûreté nucléaire pour la conception du palier 1450 MWe* (The Nuclear Safety Approach in Designing the 1450 MWe Series) by Francis Vitton, EDF/SEPTEN.

[353] See the Focus feature in Chapter 2.

[354] As is the case for the nuclear power plant fleet, the DBE may be a bounding version of the SME for the reactor sites; the same is true for the OBE in relation to the MHPE.

One of the most noteworthy aspects of combining situations is that, for certain mechanical equipment that conveys or contains pressurized fluid and has been classified as important to safety[355], the decision has been made to (quadratically) combine the loads corresponding to the design-basis earthquake (DBE) with those corresponding to situations resulting from the design-basis operating conditions (categories 1 to 4), including those involving failure of a component designed to withstand the DBE[356]. In addition, the subsequent occurrence, at the least favourable moment, of an earthquake aftershock corresponding to the operating-basis earthquake (OBE), might also need to be studied if the aftershock could adversely affect the return of the reactor to a safe state.

The term 'combination' accurately represents the type of analysis required to determine the respective chronology of events considered to occur together.

8.6. Situations to be taken into account in application of pressure equipment regulations[357]

The history of regulations applicable to pressure equipment and, more specifically, those that apply to nuclear pressure equipment used in reactors, as well as information concerning their design, are presented in Chapter 2 and Section 7.5 of this book. Some additional information is provided below[358].

Pressure equipment regulations refer to the concept of 'situations' defined in Article 7 of the Order of 26 February 1974 (currently in force), which are classified as follows:

- Category 1 situation: the situation "of the pressure equipment item if it were subjected to constant actions over time, defined on the basis of the most severe actions that the item is subject to when it is in Category 2 situations as defined below. [...] The pressure and temperature values chosen to define the Category 1 situation for each item are referred to as the design pressure and design temperature";
- Category 2 situations: "situations that the pressure equipment item is subjected to during normal operation, i.e. in continuous operation as well as during transients and common operating incidents." Normal operating transients (such as load-following) and incidents of average frequency ('simple' reactor trip, loss of

[355] Namely, engineered safety features and their support systems.

[356] Such as a pipe break in the reactor coolant system or secondary system. As stated earlier, for reactors prior to the N4 series, this combination was only applied in Category 4 situations. The study of these combined situations was specified in 1984 in fundamental safety rule RFS IV.2.a.

[357] Information gathered in collaboration with Simon Liu at ASN/DEP and Rémy Catteau at ASN/DCN.

[358] Readers can also refer to articles BN3280V1 and BN3282V1 appearing in *Techniques de l'ingénieur*, written by Jean-Marie Grandemange (†), entitled *Conception des enceintes sous pression* (Designing Pressure Vessels), parts 1 and 2, January 2008.

vacuum in the condenser, turbine trip, etc.) are classified in Category 2, and are also known as normal and upset situations;

- Category 3 situations: exceptional situations ("accident circumstances that are very infrequent but that could be envisaged", for example, total loss of steam flow in the secondary system);
- Category 4 situations: accident situations (described as 'extremely improbable', such as a main pipe break in the reactor coolant system or a main steam-line break) that necessarily entail study of the accident consequences in order to ensure that the pressure equipment item can continue to perform safely.

With regard to the classification of the design-basis situations resulting from the operating conditions used in the deterministic safety analysis, normal and upset situations include the Category 2 design-basis situations; the Category 1 situation is a conventional reference situation. Exceptional and accident situations correspond to category 3 and 4 design-basis situations. An initiating event, however, may be placed in different categories, for example, as a mechanical situation when applying pressure equipment regulations and as a design-basis situation in the context of a deterministic safety analysis.

Article 10 of the Order of 26 February 1974 set safety factors to be met by pressure equipment items (in the main primary system) of pressurized water reactors, in view of certain damage mechanisms (i.e. excessive deformation[359] and plastic instability). The manufacturer had to demonstrate that the equipment would not suffer the damage in question in situations obtained by multiplying loads in the previously defined situations by the defined safety factors (ranging from 1.1 to 2.5, depending on the situation categories defined above and the damage mechanism).

Although these factors were not included in the texts relating to nuclear pressure equipment, since they are now left for designers to assess, they are obviously still valuable as a reference that can be used by manufacturers and safety organizations to assess equipment safety in both the main primary system and main secondary system (they have been incorporated in different forms into the RCC-M code).

8.7. Assessing the radiological consequences of incidents, accidents and hazards

The nuclear safety demonstration ultimately involves an assessment of the radiological consequences of the postulated incidents and accidents and, more generally,

[359] Excessive deformation refers to significant persistent deformation that remains once the load has been removed. The load threshold corresponding to excessive deformation is the threshold at which there is a sudden increase in the variation kinetics of a characteristic dimension of the equipment for a certain increase in the load applied, i.e. where generalized yielding of the wall appears. When the load goes beyond the excessive deformation threshold, different antagonistic effects appear, but when this is no longer the case, deformation of the equipment occurs in an unstable manner, potentially leading to its 'ruin'.

of all events – including hazards – likely to affect a nuclear power reactor and lead to release of radioactive substances[360].

Assessments of radiological consequences are thus carried out from the design stage. They are updated during the periodic plant reviews as part of an overall approach aimed at reducing radioactive release and its consequences for people and the environment as far as reasonably possible.

The assessment of radiological consequences conducted as part of the safety demonstration should not be confused with assessments carried out in the context of real emergencies (in the course of emergency response) with the aim of taking action, as necessary, to protect the public (discussed in greater detail in Chapter 38).

Any assessment of radiological consequences should take into account:

– all the radioactive substances involved in the facility and their conditions of release,

– all the transfer pathways of these substances from their source of emission to people or points of interest in the environment (rivers, the sea, vegetable crops, etc.),

– all the exposure pathways for people or points of interest.

Assessments of radiological consequences must cover all time periods when environmental contamination or significant exposure could exist following the postulated accident.

There are two main stages involved in carrying out an assessment of radiological consequences: assessing any release from the facility, then assessing the radiological consequences of any release to the environment outside the facility. Assessment requires a study of local weather conditions, including wind speed and direction, groundwater and hydrogeology in general, as well as population distribution. These aspects are not discussed further in this book.

Generally, the brief explanations given hereafter concern both estimation of the radiological consequences for design-basis (or reference) operating conditions, and for complementary operating conditions (Chapter 13) or core-melt situations (Chapter 17).

[360] Article 3.7 of the Order of 7 February 2012 (the 'INB Order') explicitly prescribes the assessment of potential consequences, whether radiological or not, of incidents and accidents. ASN Guide No. 22 on the design of pressurized water reactors specifies that the radiological consequences of the reference internal and external hazards leading to radioactive release must be assessed.

8.7.1. Assessing radioactive substances released from the facility

Assessment of radioactive substances released from the facility and their properties (in terms of the types of radioactive substances [isotopes], the quantities released, and the release kinetics) relies on determination of the following:

- the types and quantities of radioactive substances present in the reactor core, system lines, spent fuel pools or tanks (effluents from the facility, etc.);
- the release rates of these substances during the situation in question: for fuel, the release rate of the various radioactive substances depends to a great extent not only on their physicochemical properties, but also the conditions to which the fuel was subjected (before the situation occurred) and is subjected to during the situation, as well as its physical state (solid or partially or completely molten);
- the modes of transfer and deposition of radioactive substances in system lines and buildings: depending on the physicochemical form in which the radioactive substances reach the systems or buildings, the conditions they encounter, their properties, etc., assessment may take into account the fact that a portion of these substances is deposited in the system lines and buildings;
- leak rates into the outdoor atmosphere and the presence of any filtration equipment: the rate at which radioactivity leaks from a building into the environment depends on the pressure it is subject to during the development of the situation in question, any installed ventilation and filtration systems, and their efficiency in the prevailing conditions. Special attention should be given to the possibility of 'direct' leaks into the environment (i.e. bypassing the confinement barriers[361]). For an accident in the reactor building, the radiological consequences calculated depend greatly on the 'direct' leak rate (because there is no filtration of release through direct leakage pathways);
- release duration, as well as emission height (this parameter must be taken into account to assess atmospheric dispersion of radioactive substances).

Analysis of the state or operability of facility systems, structures and components during the accident under study must be conducted to identify all parameters likely to have an influence on the release of radioactive substances from the facility. For each of these parameters, assumptions are made by the operator. The INB Order states that "the assumptions used to calculate any release of radioactive substances must be reasonably conservative." In some cases, sensitivity studies are carried out, varying the parameters for which there are significant uncertainties.

The assessment of release from the facility during an incident, accident or hazard is conducted on the basis of the deterministic analysis described above. Applicable

[361] The risk of containment being bypassed in core melt situations is discussed in Chapter 17.

methods and study rules are taken into account accordingly (consideration of an aggravating event, combination with a loss of off-site power, operator response time, etc.). If a specific thermal-hydraulic study is necessary to characterize release (as in the case of a loss-of-coolant accident, as opposed to an assessment covering only the rupture of a tank containing radioactive substances), it should be consistent with the thermal-hydraulic study of the situation (assumptions relating to the scenarios studied, etc.). Finally, facility-related assumptions taken into account in the assessment of radiological consequences must be consistent with the assumptions and safety requirements featured in the safety analysis report (requirements related to design, classification, etc.) and the general operating rules (such as the maximum leak rate from the containment in accident situations).

Radioactive substances can be released into the atmosphere in gaseous or aerosol form and to surface water in liquid form. Measures should be taken at the facility design stage to prevent[362] them from reaching groundwater.

As a general rule, it is assumed that when the fuel rod cladding is not leaktight, rare gases (xenon, krypton) completely escape into the reactor coolant system and from the reactor coolant system into the reactor building, with no retention (if fuel melting does not occur, only the rare gases in the gap between fuel pellets and cladding are considered).

This is not the case for the other radioactive substances. With iodine[363], a major contributor to short-term radiation exposure of the public during accidents affecting nuclear power reactors, different aspects need to be taken into consideration:

- its physicochemical form: gaseous molecular form (I_2), particulate form (i.e. aerosol, such as caesium iodide, CsI), gaseous organic form (such as iodomethane, CH_3I); organic iodine is the most difficult to retain using existing filtration systems;
- the phenomena or mechanisms likely to lead to iodine transformation, trapping or deposition, depending on its physicochemical form.

In particular, in the containment of a pressurized water reactor, gaseous iodine in its molecular form is rapidly adsorbed by paint on the walls or paint on equipment inside the containment, forming gaseous organic iodine; under the effect of radiation, this iodine in organic form may then turn into iodine oxides, considered as very small particulates.

When the containment spray system operates (loss-of-coolant accident, core-melt situations), the spray will draw gaseous iodine in molecular and aerosol form into

[362] Experience feedback shows some groundwater contamination, particularly by tritium; but this is not due to operating conditions or hazards at the facilities concerned, but rather a leaktightness failure.

[363] On this subject, see Nuclear Power Reactor Core Melt accidents. Current State of Knowledge, D. Jacquemain *et al.*, Science and Technology Series, IRSN/EDP Sciences, 2013, especially Section 4.3.1.6.

the sumps, where the aerosols can enter into complex chemical reactions, ultimately producing gaseous iodine in molecular form.

These very complex subjects will not be discussed further.

8.7.2. Assessing radiological consequences of radioactive release from the facility

The radiological consequences of release from the facility are assessed in several steps:

- appropriate characterization of the site environment (topography, land use, hydrology, meteorology, etc.);
- identification of the population and points of interest in the environment (such as agricultural production and water resources) likely to be affected by the release of radioactive substances; the population may be described at this point as persons representative[364] of the most exposed homogeneous groups;
- identification of the transfer pathways of the radionuclides into and within the environment and characterization of the state of contamination of the 'representative persons' (including through ingestion of contaminated foodstuffs) and the environment (agricultural production, water resources, etc.), as well as the exposure of these persons to direct radiation;
- calculation of the consequences in terms of dose received, including identification of the exposure pathways of the 'representative persons' and assessment of dose indicators expressed as effective dose or equivalent dose that could be received by these persons (dose to the thyroid in particular).

It is important to note that the transfer pathways of radionuclides in the environment and exposure pathways for people may differ depending on the phase of the accident, the change in contamination over time, the weather and other factors.

The INB Order stipulates that assessments must include estimates of the doses that people could be exposed to in the short, medium and long term. The timescale is defined taking into account release kinetics and all the resulting phenomena in terms of environmental contamination or radiation exposure of the population.

In the case of radioactive release into the atmosphere, four radiation exposure mechanisms may be observed more or less simultaneously:

- release of gaseous elements, particularly rare gases,
- release in the form of aerosols,
- ground deposits, with a distinction made between:

[364] For more details on this concept, see ICRP Publication 101a, Assessing Dose of the Representative Person for the Purpose of Radiation Protection of the Public, Elsevier, 2006.

- deposits consisting of short-lived radioactive elements (typically with a half-life of about ten days, such as iodine-131), which have an impact on the environment and people that is limited to a few weeks or months;
- deposits of longer-lived elements (such as caesium-137, plutonium-239 and others) which can persist in the environment for a period that exceeds human lifetime.

In view of the characteristics of these mechanisms, different time periods can be identified when assessing the radiological consequences of radioactive release.

Transfers of radioactive substances into the atmosphere obviously depend on weather conditions. Assumptions must therefore be made regarding wind speed and direction, the axial gradient of air temperature (which determines atmospheric dispersion) and precipitation. In France, for a long time assessments were conducted using abacuses (such as those developed in the 1970s and 1980s by R. Le Quinio and A. Doury), which provide atmospheric transfer coefficients for different sets of weather conditions. The development of powerful simulation software now makes it possible to produce more accurate assessments very quickly.

The altitude of release should also be taken into consideration. Release assumed to be at ground level is likely to maximize the radiological consequences over short distances (the 'near field' effect).

8.7.3. Assessing radiological consequences

Assessments of radiological consequences help to verify the suitability and adequacy of risk control measures, during the (generally iterative) design studies of a new reactor, or during studies for changes or periodic reviews. These assessments form part of a continuous improvement approach to safety, aimed at reducing radioactive release, as well as its impact on humans and the environment, as far as reasonably achievable.

With this in mind, the results of assessments of radiological consequences may be 'situated' in relation to radiological targets set by the operator (see Sections 6.2 and 8.1). However, as emphasized earlier, **the fact that radiological targets are met does not, on its own, determine the adequacy of design or improvement measures. On the one hand, some safety measures cannot be evaluated by assessing radiological consequences, and on the other, the approach of reducing radiological consequences to values that are as low as reasonably achievable should always be taken under any circumstances.** The final assessment can therefore only be achieved on a case-by-case basis, taking into account uncertainties.

Appendix. List of EPR (Flamanville 3) reference transients, incidents and accidents involving the reactor and spent fuel pool

The study of certain transients, incidents and accidents below was carried out for specific reactor states (or areas of study), graded A to F (in brackets), which are defined at the end of this appendix (see also Section 20.2.1.1).

▶ PCC 2 reference transients

- spurious reactor trip [state A];
- feedwater system malfunction causing a decrease in feedwater temperature [states A, B];
- feedwater system malfunction causing an increase in feedwater flow [states A, B];
- excessive increase in secondary steam flow rate [state A];
- turbine trip [state A];
- loss of condenser vacuum;
- short-term loss of off-site power (≤ 2 h) [states A, C, D, E];
- loss of normal feedwater flow (loss of all the main feedwater pumps and the startup and shutdown pump);
- loss of one reactor coolant pump without partial reactor trip;
- inadvertent control RCCA bank withdrawal [state A];
- incorrect position of a control RCCA up to rod drop, without taking into account ‘limitation’ systems;
- startup of an inactive reactor coolant loop at an incorrect temperature [state A];
- malfunction of the chemical and volume control system that results in a decrease in boron concentration in the reactor coolant [states A to E];
- malfunction of the chemical and volume control system causing an increase or decrease in the reactor coolant inventory;
- primary side pressure transients (spurious pressurizer spraying, spurious pressurizer heating);
- uncontrolled reactor coolant system level drop [states C3, D, E];

- loss of one cooling system train in shutdown [states C3, D, E];
- loss of one RWST cooling train or an RWST support system [state A].

▶ PCC 3 reference incidents

- small break (DN ≤ 50 mm) in a steam generator feedwater system pipe or steam pipe, including breaks in lines connected to steam generators (DN ≤ 50 mm) [states A, B];
- long-term loss of off-site power (> 2 h) [state A];
- inadvertent opening of a pressurizer safety valve [state A];
- inadvertent opening of a bypass valve or safety valve on a steam generator [state A];
- small-break loss-of-coolant accident [states A, B];
- rupture of one steam generator tube [state A];
- inadvertent closure of one or all of the steam isolation valves;
- core nonconformity (inadvertent loading and operation of a fuel assembly in an incorrect position);
- forced decrease of the reactor coolant flow rate (4 pumps);
- failures in liquid or gaseous waste treatment systems;
- inadvertent control RCCA bank withdrawal [states B, C, D];
- inadvertent RCCA withdrawal at power;
- rupture of a line carrying reactor coolant outside the containment (e.g. nuclear sampling line);
- loss of power (> 2 h) for spent fuel pool cooling in fuel building [state A];
- loss of an RWST cooling train or an RWST support system [state F];
- rupture of an isolatable pipe in a system line connected to the spent fuel pool [states A to F].

▶ PCC 4 reference accidents

- long-term loss of off-site power (> 2 h) [state C];
- steam-line break;
- feedwater line break;
- inadvertent opening of a bypass valve or safety valve on a steam generator [state B];
- control RCCA ejection [states A, B];

- intermediate-break or large-break loss-of-coolant accident [states A, B];
- small-break loss-of-coolant accident (DN ≤ 50 mm) [states C, D, E];
- reactor coolant pump failure (rotor seized);
- reactor coolant pump shaft break;
- rupture of two tubes on one steam generator [state A];
- fuel handling accident;
- boron dilution due to a non-isolatable rupture on a heat exchanger tube [states C to E];
- isolatable break in the residual heat removal system inside or outside the containment (DN ≤ 250 mm) [states C, D, E];
- non-isolatable small-break loss-of-coolant accident (DN ≤ 50 mm) or isolatable break in the residual heat removal system (DN ≤ 250 mm), pool draining [state E];
- multiple system failures in the nuclear auxiliary building (NAB) and the effluent treatment building (ETB) in an earthquake situation.

This list of transients, incidents and accidents makes reference to reactor states and substates, defined as follows in the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors:

- State A: power state as well as hot or intermediate shutdown state with all the automatic reactor protection functions available; certain functions may be deactivated at low pressure.
- State B: intermediate shutdown with reactor coolant system water temperature above 120°C, residual heat removal system not connected; some automatic reactor protection functions may be deactivated.
- State C: intermediate and cold shutdown, with the residual heat removal system in operation and the reactor coolant system closed or ready to be rapidly reclosed. The substates in group C3, which appears in the above list, are situations in which the main primary system is closed with the water level "between pressurizer full and ¾ loop level", or the main primary system is partially open (as a minimum the pressurizer vent line is open) and the water level is "greater than or equal to ¾ loop level"); in these situations, 3 out of 4 trains of the RIS-RHR system are in operation, i.e. connected to the main primary system.
- State D: cold shutdown with the reactor coolant system open.
- State E: cold shutdown with the reactor cavity flooded.
- State F: cold shutdown with the reactor core completely unloaded.

Chapter 9
Loss-of-Coolant Accident

This chapter describes the physical phenomena involved in a loss-of-coolant accident (LOCA) and the assumptions posed in studies on this event. A loss-of-coolant accident results from a pipe break in the reactor coolant system of a pressurized water reactor (shown in Figure 9.1) and is fundamental in designing the essential parts of a pressurized water reactor, specifically the engineered safety systems (safety injection system [SIS] and containment spray system[365] [CSS]). Starting in the 1970s, this accident was the focus of most early nuclear safety research, aimed at acquiring the knowledge and simulation software necessary to study this event.

Reactor coolant system breaks also serve to design the many equipment items that may be subject to the mechanical effects of ruptures and must withstand these effects without aggravating the accident situation. These equipment items are:

- the nuclear steam supply system (the vessel and its internals, other pipes and their support systems),
- fuel assemblies,
- the containment and its internals, including the reactor pit and the reactor coolant system bunkers containing the heavy equipment of the reactor coolant system (pumps, steam generators, pressurizer).

[365] Not featured on the EPR, which has a spray system (CHRS) designed to be used for core-melt situations only.

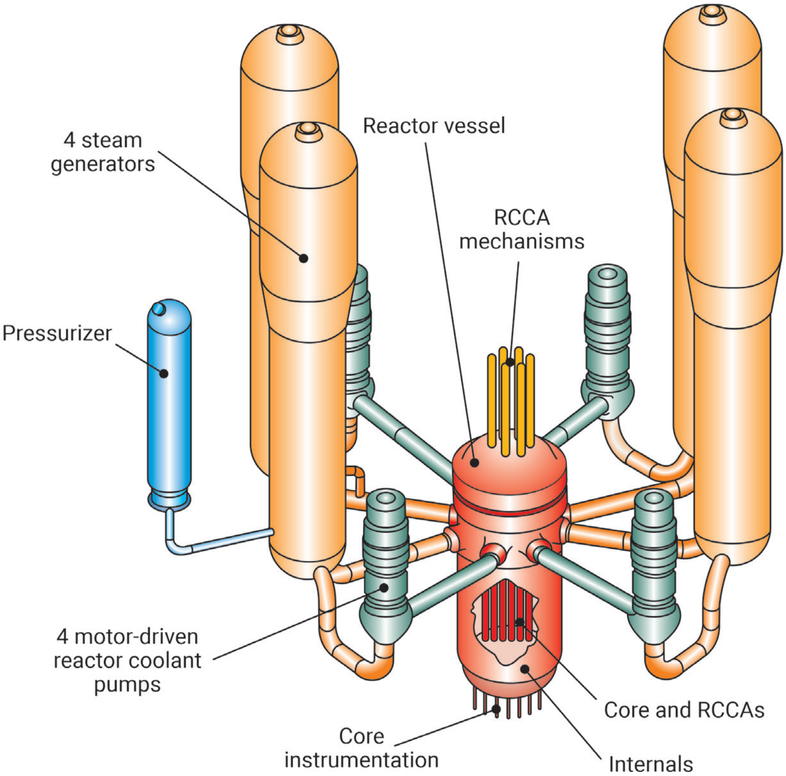


Figure 9.1. Reactor coolant system of a pressurized water reactor. Georges Goué/IRSN.

The breaks chosen for design purposes determine the qualification requirements applicable in degraded ambient conditions for equipment in the containment that is necessary during and after the accident (qualification in accident conditions), such as the SIS and CSS.

Since the beginning of civil use of nuclear energy in the USA, with the first pressurized water reactor built by Westinghouse at the end of the 1950s[366], the loss-of-coolant accident has been postulated as a 'maximum credible accident'. This accident was studied to evaluate the potential releases and radiological consequences occurring near the power plant in the event of a cladding failure during such an accident, as a criterion for selecting the power plant site. These considerations led to the design principle (along with the associated rules and criteria) requiring that a pressurized water reactor must withstand the effects of a loss-of-coolant accident.

The occurrence of a pipe break in the reactor coolant system leads to a pressure drop and loss of water in the system.

[366] Shippingport pressurized water reactor, commissioned in 1957.

The pressure drop results in significant mechanical loads on the vessel internals and fuel assemblies which must nevertheless maintain their functions to ensure reactor shutdown by dropping neutron-absorbing rods into the core and providing core cooling capacity, while maintaining assembly geometry.

The water lost via the break may also lead to partial or total core uncovery. This may damage the fuel rods, resulting in loss of leaktightness or even mechanical rupture of some of them. This damage must remain limited so that the core cooling capacity is not compromised and the radiological consequences of the accident are also limited. The water from the reactor coolant system spills into the containment with part of the water from the safety injection system, leading to vaporization and thus a significant increase in the containment pressure and temperature. Some containment equipment will then be in 'degraded ambient conditions', which must be taken into consideration in the equipment qualification requirements.

For these reasons, the LOCA was taken into account in the design phase for pressurized water reactors, in designing or verifying the design of important reactor equipment, especially vessel internals and fuel assemblies, the safety injection system (SIS) (including the accumulators), the reactor containment, and the containment spray system (CSS). These studies also established the maximum permissible linear power density of the fuel rods at each point of the core in normal operation, which determines the maximum temperature the fuel rod cladding can reach during the accident.

The sequence and consequences of a LOCA are directly related to the location and size of the break. The spectrum of potential breaks in the reactor coolant system ranges from those that can be compensated by the charging flow rate of the chemical and volume control system (CVCS), to a break in a main pipe of a reactor coolant loop, with complete separation of the two parts and double displacement of the two ends (in a break perpendicular to the axis of the pipe, called a '2A guillotine' break, where A is the pipe's cross-sectional area).

On one hand, cold leg breaks constitute the worst-case scenario in terms of the risk of losing core cooling capacity. This situation leads to partial loss, through the break, of the SIS water injected into the cold leg of the ruptured loop, which does not contribute to core cooling. On the other hand, hot leg breaks are the worst-case scenario for reactor containment resistance, given the high temperature of the fluid exiting the break, resulting in higher pressures.

From the design phase of the first pressurized water reactors in the French nuclear power plant fleet, a spectrum of breaks up to the 2A break was systematically postulated to study certain consequences of a LOCA (thermal-hydraulic studies: core cooling capacity, containment strength, radiological consequences). Other consequences (mechanical strength of vessel internals and fuel assemblies) were only studied for breaks with limited displacements. In all the reactors in the French nuclear power plant fleet up to the 1450 MWe series (N4), anti-whip restraints for limiting pipe displacements in the event of a break or an earthquake were installed and taken into consideration in the mechanical studies. Eleven conventional locations of reactor coolant pipe ruptures were taken into account in these studies. Conventionally, these ruptures are all assumed to occur almost instantly (opening in one millisecond). One of them is longitudinal, the others are referred to as guillotine breaks (i.e. perpendicular to the axis of the pipe). For the postulated rupture at the outlet of a reactor coolant pump, where there are no anti-whip restraints, the stiffness of the cold leg is taken into consideration in the studies, which leads to limiting the cross-sectional area of the corresponding break.

This approach was based on the US licence. The breaks were selected according to mechanical criteria, in areas of the reactor coolant system subjected to the most stress. Some aspects of the US approach are mentioned in Section 9.2.1.

A new baseline for the study of LOCAs[367] was defined in France in 2010-2014, in particular to harmonize the break spectra used in mechanical studies and thermal-hydraulic studies (the same breaks are now studied in both) and to take into account phenomena brought to light by R&D studies and other work on this type of accident. In this context, Électricité de France (EDF) proposed a new LOCA study method, described in Section 9.2.2. This new method takes into account physical phenomena related to fuel behaviour not previously considered.

The Flamanville 3 EPR design differs from previous French reactors in that it applies a pipe break exclusion principle for the main primary system[368], provided the pipes have a specific design and are inspected appropriately. In these conditions, only nozzle ruptures on the most important lines connected to the reactor coolant system are examined in design-basis (or reference) LOCA studies. As a result of applying rupture exclusion, reactor coolant pipework does not have anti-whip restraints.

9.1. Short- and medium-term aspects of a LOCA

This section describes the short- and medium-term consequences of a LOCA for the nuclear steam supply system, fuel assemblies and rods, and the containment.

The sequence and consequences of this type of accident are directly related to the location and size of the break.

As indicated above, for the thermal-hydraulic study, the spectrum of potential breaks in the reactor coolant system ranges from breaks that can be compensated by the charging flow rate of the CVCS to the complete rupture of a main pipe, called a 2A rupture.

LOCA transients occur following postulated breaks in the reactor coolant main pipework, with diameters between 1 and 14 inches for 'intermediate breaks' (IB) and greater than 14 inches for 'large breaks' (LB). The maximum break size corresponds to the double-ended guillotine break of a reactor coolant pipe.

[367] A set of assumptions, rules and criteria, and study methods.

[368] This principle is also used for the main secondary system pipework of the Flamanville 3 facility.

Location	Cold leg	U leg	Hot leg
Diameter Ø (inches)	27.5	31	29
Area 2 x A (cm^2)	7664	9739	8522

As mentioned above, for mechanical strength studies of vessel internals and fuel assemblies, only breaks with limited displacements were considered. The diameter of the largest break used is 16 inches (rather than nearly 30 inches, not including anti-whip restraints).

Intermediate Breaks (IB), with an equivalent diameter greater than 1 inch, and Large Breaks (LB) are studied as Category 4 operating conditions.

The initial focus of the studies was large breaks. After the accident at the Three Mile Island nuclear power plant, they began to focus on intermediate breaks.

9.1.1. Mechanical effects on vessel internals and fuel assembly structures

For breaks that are large enough, pressure at the break decreases almost instantly and reaches the local saturation pressure. This local decompression, ranging from 50 to 80 bars, propagates as a decompression wave in the reactor coolant system at the speed of sound in water (about 1000 m/s), gradually accelerating the flow of coolant to the break.

For a break in the cold leg, the arrival of the wavefront in the vessel causes an asymmetric depression in the vessel inlet downcomer that results in very significant lateral forces on the core barrel and the internal wall of the vessel. As the decompression wave propagates to the inside of the vessel, toward the core, the associated pressure and flow rate variations cause very rapid, alternating variations in the vertical hydraulic forces on the vessel internals and fuel assemblies, as well as forces due to pressure differences on the upper support plate and the core baffle (see Figure 9.2). Since these two structures have calibrated orifices that limit the rate of core bypass, pressure drop in the areas they delimit occurs more slowly than in the reactor coolant system.

In the case of a hot leg break, the decompression wave first penetrates the vessel by its outlet manifold, delimited by the upper plate of the core and the upper support plate equipped with RCCA guide tubes. These plates are interconnected by support columns (see Figure 9.2). The RCCA guide tubes and the columns are then subjected to horizontal forces, causing them to buckle[369]. The wave goes on to propagate from the top to the bottom of the core then to the annular downcomer, causing vertical force variations on the fuel assemblies and vessel internals. A wave also arrives in the

[369] Buckling is an instability phenomenon in an elastic structure that, to avoid an overload situation, 'uses' a mode of deformation that offers less stiffness under loading. The structure, subjected to a compression force along an axis, will tend to bend and deform perpendicularly to the compression axis.

vessel via the cold leg of the ruptured loop. It leads to forces qualitatively similar to those of a cold leg break, but they are 'smoothed' because of the many layers of waves transmitted and reflected along the reactor coolant loop as it passes through the large components of the reactor coolant system.

Thus, the consequences of a break under hydraulic forces differ in amplitude and direction relative to the initial flow, depending on the rupture location.

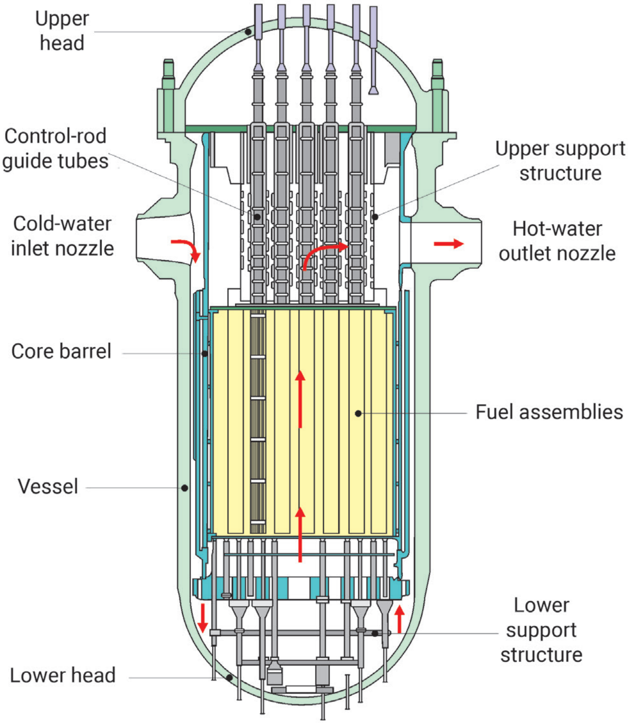


Figure 9.2. Vessel internals of a pressurized water reactor. Georges Goué/IRSN Media Library.

The vessel internals dynamically 'respond' to the variation of the hydraulic forces applied over time. In particular, the horizontal movements of the lower and upper core plates apply stress to the fuel assemblies which they secure by means of pins. These movements may cause colliding between the assembly grids themselves and colliding between the peripheral grids and the core baffle, resulting in a risk of buckling that could compromise core geometry and prevent coolant circulation through the core. Given the variation of vertical forces on the fuel assemblies, it is necessary to ensure that they always remain vertical.

These various effects are examined in mechanical behaviour studies on vessel internals and fuel assemblies in order to demonstrate their ability to withstand LOCA conditions.

9.1.2. Thermal-hydraulic aspects and behaviour of fuel rods

The thermal-hydraulics of a LOCA situation and the behaviour of fuel rods depend on the size of the break. The descriptions below make a distinction between specific features of large breaks and intermediate breaks, which are shown schematically in Figure 9.3. As indicated above, the vast majority of research and development studies on fuel behaviour in the event of a LOCA situation[370] initially focused on large breaks.

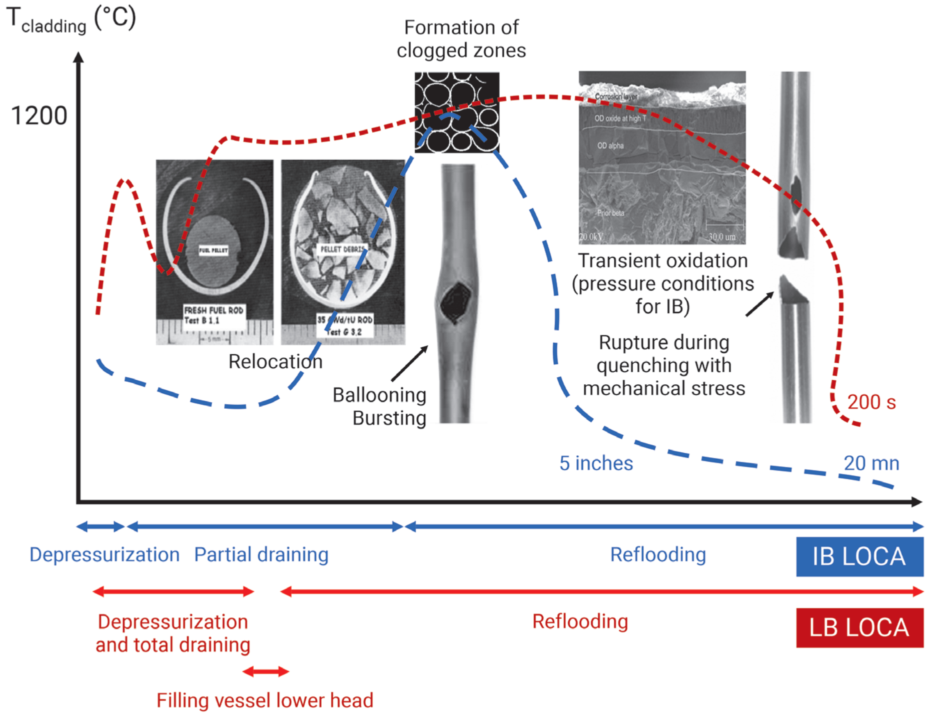

T_{cladding} (°C)
1200
Formation of clogged zones
FUEL PELLET
FRESH FUEL ROD Test B 1.1
PELLET DEBRIS
35 GWd/tU ROD Test G 3.2
Relocation
Ballooning Bursting
Transient oxidation (pressure conditions for IB)
Rupture during quenching with mechanical stress
200 s
5 inches
20 mn
Depressurization
Partial draining
Reflooding
IB LOCA
Depressurization and total draining
Reflooding
LB LOCA
Filling vessel lower head

Figure 9.3. Behaviour of fuel assembly rods in a LOCA situation, depending on the size of the break in the reactor coolant system, with corresponding thermal-hydraulic phases. IRSN.

9.1.2.1. Large-break LOCA

This type of transient is fast, lasting about 200 s. It leads to a sudden pressure drop in the fluid of the reactor coolant system, leaving the core completely uncovered.

From a thermal-hydraulic point of view, this accident scenario can be broken down into three phases: depressurization and total draining, filling the vessel lower head, and reflooding the core.

[370] On this subject, readers may also refer to the book Current State of Research on Pressurized Water Reactor Safety by J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017, Chapter 3.

Once the break opens, which is assumed to happen almost instantly, the reactor coolant system rapidly drains into the containment, leading to a reactor trip, then startup of the safety injection system when the very low pressure threshold is reached in the pressurizer. After the pressure in the reactor coolant system falls below 40 bars (in about 20 s), the accumulators, which are tanks of borated water pressurized using nitrogen, passively inject water into the vessel. At the end of depressurization, an SIS low-pressure pump takes over to ensure water injection.

Although neutron production is halted by the 'void effect' (due to the reactor coolant which acts as the neutron moderator – see Section 5.2) and the neutron-absorbing rods are dropped, the fuel assembly rods continue to release heat (referred to as 'decay heat'). Since only steam is passing through the core, heat exchange between the cladding and the fluid is very low. Rod cladding temperature rises very fast, reaching values above 700°C.

Due to depressurization of the reactor coolant system, internal fuel rod pressure may exceed the pressure in the reactor coolant system. Under the combined action of increased cladding temperature (1 to 30°C/s) and the pressure difference between the inside and outside of the rods, the rods may deform by ballooning and eventually burst.

If the cladding bursts, fuel fragments may accumulate in the ballooned burst area of the rod. This phenomenon, called fuel relocation, significantly changes the local power generated at the ballooned burst area of the fuel rods and tends to locally increase their temperature.

Finally, fuel rod ballooning and bursting leads to partial clogging of the fuel assembly hydraulic channels. Under certain conditions (including axial extension of the clogging), this may compromise core cooling capacity by limiting fluid circulation.

From a physical-chemical perspective, the zirconium-based alloys oxidize rapidly in the presence of high-temperature steam, producing hydrogen. The oxidation reaction is exothermic and its kinetics are an exponential function of the temperature. The expression 'transient oxidation' is used to make a distinction between this phenomenon and oxidation that occurs during normal reactor operation.

The steam that penetrates the burst fuel rods incorporates hydrogen as the rod cladding oxidizes. The hydrogen thus released is absorbed to a significant extent by the cladding's inner surface, a phenomenon called 'secondary hydriding' that makes the cladding brittle.

Due to the thermal shock resulting from the reflooding phase (characterized by cooling kinetics between 10 and 100°C/s), the fuel rods, embrittled during 'transient oxidation', undergo significant thermal stresses, potentially causing their rupture or even fragmentation. In addition to these thermal stresses from quenching, there may also be other mechanical loads resulting from rods being blocked in the grids, for example.

At the end of the transient, the core is cooled and the cladding temperature is about 135°C (close to the temperature of the fluid at saturation in the reactor coolant system at a pressure of a few bars).

9.1.2.2. Intermediate-break LOCA

This type of transient is slower than the large-break LOCA (from a few minutes to 30 minutes, depending on the size of the break and the assumptions made regarding operation of the reactor coolant pumps – RCPs). Core uncovery, in two-phase conditions (liquid and steam), is more or less deep.

For small intermediate breaks (diameter less than 4 inches), residual heat is mainly removed by the steam generators. The pressure in the reactor coolant system then stabilizes at a value slightly higher than the pressure in the secondary system, set by its discharge valves (about 80 bars). For intermediate breaks with a diameter greater than 8 inches, the residual heat is removed through the break, resulting in a faster pressure drop in the reactor coolant system, which rapidly reaches a few bars.

Intermediate breaks cause thermal-hydraulic phenomena that differ noticeably from those resulting from large breaks because the heat sink (steam generators) continues to play a substantial role in removing residual heat. Due to low flow rates, significant stratification phenomena are observed between the liquid and the steam. The accident scenario can be broken down into three main phases: liquid single-phase depressurization, reduction of the water inventory, and filling of the reactor coolant system by water injection from the accumulators and the SIS.

The larger the break size, the more the accident sequence resembles a large-break LOCA (particularly for breaks with a diameter greater than 10 inches).

In addition, an intermediate-break LOCA may, in certain parts of the reactor coolant system, lead to the formation and accumulation of slightly borated water due to steam condensation in the steam generator tubes. In this situation, since the accident procedures call for the operator to start cooling using the steam generators, natural circulation may return in the reactor coolant system with the transfer of slightly borated water 'slugs' to the core. This presents a risk of power excursion and uncontrolled criticality in the reactor. This phenomenon is often referred to as 'dilution inherent to a LOCA', and is covered in a specific study.

While the physical phenomena in an intermediate-break LOCA resemble those in a large-break LOCA, behaviour of the fuel assembly rods is not the same. In an intermediate-break LOCA, the kinetics of temperature rise and cooling are slower (about 10°C/s) than in a large-break LOCA. Furthermore, in an intermediate-break LOCA, transient oxidation occurs at a higher pressure (between 20 and 40 bars) than in a large-break LOCA.

The maximum fuel rod temperature is not necessarily a monotonic function of the break size. Rather, the break size and location, together with the study assumptions used, influence the calculated thermal-hydraulic behaviour of the reactor and thus the maximum cladding temperature.

9.1.3. Effects on reactor containment and internals

Water from the reactor coolant system that has spilled into the containment and part of the water from the safety injection system that may (or may not) have cooled the fuel and the structures leads to vaporization and thus a significant pressure and temperature increase in the reactor building.

LOCA consequences are therefore used to size the containment and its internal structures and determine the pressure and temperature profiles to be used to qualify the equipment required in accident conditions (see Section 7.4.3).

Internal containment structures consist of the reinforced concrete floors and walls that separate the reactor coolant loops from each other and serve as biological shielding. These structures form compartments or bunkers containing the large components of the reactor coolant system, which are anchored in the walls of the bunkers. The vessel, in particular, is suspended in the cylindrical reactor pit by a support ring anchored at its rim.

Since the coolant released by the break spills into the compartments closest to the rupture, in the short term their walls are subjected to pressure differences between adjacent compartments and to the impact of the jet of water and steam from the break. The hydraulic forces inside the reactor coolant system that are transmitted to the component support structures must be borne at the anchors in these walls. In addition, the rupture of a reactor coolant loop must not aggravate the rupture, nor lead to rupture of another loop (non-aggravation of the accident).

In the specific case of a rupture at a vessel inlet or outlet nozzle, the reactor pit is temporarily and asymmetrically pressurized, which creates lateral forces on the outer wall of the vessel. The vessel is also subject to a vertical force due to the fact that pressure in the reactor pit increases faster than pressure in the rest of the containment, which acts on the reactor vessel head. These forces, combined with the hydraulic decompression forces and the mechanical forces transmitted to the vessel by the lower internals and the fuel assemblies, are ultimately applied to the vessel support structures.

Concerning the containment, an initial pressure peak is reached at the end of reactor coolant system depressurization. The energy absorbed by steam condensation on the walls leads to decreased pressure and temperature in the containment. Depending on the size of the break and its location in the reactor coolant system, the kinetics of the accident and its consequences in terms of pressure and temperature may vary. For a large break in the cold leg, the steam produced due to fuel rod rewetting may cause pressure and temperature to rise again and lead to a second pressure peak of lesser amplitude than the first.

For the 900 MWe, 1300 MWe and 1450 MWe (N4) reactors, the containment spray system (CSS) automatically starts when pressure in the containment exceeds a given threshold. After its startup, temperature and pressure in the containment decrease almost continuously. For the EPR, in which spraying does not occur during a LOCA, the robustness of the civil works and the large volume of the containment structure make it possible for the civil works to withstand the thermal-mechanical loads resulting from a LOCA (nozzle ruptures).

This means that containment undergoes not only one or two internal pressure peaks, but also thermal stresses that develop more slowly as the temperature front advances through the concrete.

9.1.4. Long-term aspect

At the time of the accident, the energy present in the reactor core (decay heat), in the cooling water and in the structures of the reactor coolant system is removed to the containment in the form of hot water and steam at a pressure of a few bars. In this configuration, the core is cooled by the safety injection system and the containment by the spray system. These two systems are initially supplied directly from the water tank provided for this purpose (RWST). When this tank is empty, they are connected (automatically) to the containment sumps that collect the water from the break, and thus continue to operate by 'recirculation'. The fluid recovered in the sumps is reinjected in the core by the safety injection system and is cooled by the heat exchangers before being sprayed in the containment by the spray system.

The recirculation phase may last a very long time, i.e. months or even years.

During the long-term phase of a LOCA, another effect of the break must be considered during design: the break produces debris that is entrained to the sumps (thermal insulation components around the pipes with fibrous, microporous structures, paint residues, etc.). Water recirculation may be disrupted by this debris. It may clog the water intakes and screens in the sumps (by creating fibrous debris 'beds' there); it may also damage pumps downstream of these screens by cavitation (SIS and CSS pumps). Entrainment of debris in the water recirculation loop can lead to degraded cooling at the heat exchangers associated with the CSS, as well as obstruction of the water spray header nozzles in the containment, and clogging of cooling channels in the fuel assemblies.

The risks of impeding recirculation of cooling water due to sump screen clogging in water reactors were identified in the 1970s during work on risk prevention. They were specifically covered in Regulatory Guide RG 1.82 released in 1974 by the U.S. NRC. During the early 1990s, however, several incidents occurred in boiling water reactors (at the Barsebäck plant in Sweden and at the Perry and Limerick plants in the USA), which raised new questions on the risk of screen clogging, particularly the amount of debris potentially produced in the event of a break in a pressurized water pipe.

Studies and R&D undertaken led to a significant reduction in the MICROTHERM®[371] fibrous insulating material used in the entire French nuclear power plant fleet

[371] If destroyed, this type of insulating material causes the entrainment of very small particles (about 1 mm). However, to maintain the same thermal insulation performance, the new insulating materials appear to generate a larger quantity of fibres, although larger in size. In addition, EDF has begun gradually replacing glass wool insulating materials with other materials having different characteristics.

(a change implemented from 2011 to 2018), as well as the installation of new screens (from different manufacturers) in the sumps and larger screen surface areas (a change applied from 2005 to 2009) – see Sections 29.2.2.3 and 18.2.4 concerning the EPR. R&D has been conducted and is ongoing in these areas[372]. In 2014, the French Nuclear Safety Authority (ASN) asked EDF to address all the unresolved questions involved in core cooling in recirculation mode for the fourth ten-yearly outage of the 900 MWe units, taking into account the actual state of the facilities (types of insulating materials present, etc.) and the knowledge gained from research and development work. Aside from the risks mentioned above, chemical effects have yet to be investigated. This involves effects potentially caused by the presence of boric acid, sodium hydroxide, and dissolved compounds from the debris that could affect the risks of clogging not only on sump screens, but also inside the fuel assemblies.

The long-term phase of a LOCA also involves two other risks, related to boron. The water in the reactor coolant system and in the refuelling water storage tank contains boron, in the form of boric acid. Boric acid is not entrained to the break by the steam produced in the reactor core and its solubility is limited. There is thus a risk of gradual build-up of the boron concentration in the core that could ultimately cause boron crystallization, which would block the circulation of liquid in the cooling channels of the fuel assemblies. When safety injection occurs in the recirculation mode, the boron concentration tends to decrease in the water inside the sumps, which receive the fluid released at the break (the steam does not contain boron), and to increase in the core. This leads to a risk of a return to criticality in the core, if the boron concentration drops too low in the sump water that is injected into the core.

In the event of a hot leg break on a reactor coolant loop, the safety injection water first passes through the core, and the water and steam mixture flowing out of the break carries boron in the liquid part of the flow. This avoids the risks of decreased boron concentration in the sump water and increased boron concentration in the water of the reactor coolant system. Conversely, in the event of a cold leg break, part of the safety injection water is directly released at the break, while another part is vaporized after passing through the core. Then it passes through the steam generators and the reactor coolant pumps before part of it (with a low boron concentration) flows out of the break. The risks of boron crystallization in the vessel and decreased boron concentration in the sumps therefore concern the cases of breaks on cold legs.

[372] For this purpose, EDF has conducted a series of tests including qualification tests on new sump screens, qualification tests on paints in accident conditions, tests using the CEMETE loop to study debris transfer between the areas upstream and downstream of the screens (including the chemical effects on the screens), and tests on fuel assembly clogging (at the nozzles and grids) in an Areva (Framatome) experimental loop in Erlangen in Germany. The tests conducted by IRSN, particularly using the VIKTORIA loop in Slovakia, are briefly mentioned in Section 39.2. Readers may also consult Current State of Research on Pressurized Water Reactor Safety by J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017, Chapter 5.

To avoid these penalizing phenomena in the event of a cold leg break, the operator must[373] simultaneously send safety injection water into the hot and cold legs to dilute the boron in the core while continuing to remove decay heat.

Lastly, in the long term, the containment could be subject to overpressure due to the explosion of a mixture containing hydrogen and oxygen. Oxygen is present in the air inside the containment and hydrogen is released from the following sources:

- low amounts of dissolved hydrogen in the reactor coolant system water present in normal operation to 'neutralize' radiolysis of water in the reactor core,
- a reaction between zirconium and water during the accident,
- radiolysis of the water in the sumps, due to radiation from the radioactive products it contains after the accident.

In the conditions of this design-basis or reference accident, the risk of deflagration is related to the high concentration of hydrogen that may result from radiolysis in the sumps. This risk is nonetheless avoided with the passive hydrogen recombiners featured on the reactors (for core-melt accidents, see Section 17.5.4).

9.2. Safety demonstration

9.2.1. General information and background

Generally, in the safety analysis reports for the pressurized water reactors of the French nuclear power plant fleet, the objectives to be met (such as the core cooling capacity) are indicated for each design-basis operating condition. These objectives are translated into safety requirements relevant to the postulated physical phenomena. Compliance with these requirements is then ensured by checking the technical acceptance criteria, which are calculable parameters that represent the postulated physical phenomena as closely as possible.

In France, the baseline[374] for the study of LOCAs was for a long time directly inspired by US regulations adopted in the 1970s, with the first reactors of the fleet built under a Westinghouse licence. The US baseline is given in the Code of Federal Regulations 10 CFR 50.46. This baseline defines the maximum break size for sizing the safety injection system. The maximum break size, referred to as the 'reference break', is a doubled-ended guillotine break (2A)[375], located anywhere on the main pipes of the reactor coolant system. In the beginning of the 1980s, the U.S. NRC considered the possibility of using an approach that ultimately consisted of foregoing the study of the dynamic effects caused by pipe breaks on structures and equipment, an approach referred to as 'Leak-Before-Break' (LBB). This led to the 1984 publication of

[373] Studies conducted to define when the operator is to implement this simultaneous injection generally recommend four to six hours after the safety injection has been triggered.

[374] A set of assumptions, rules and criteria, and design methods.

[375] See Appendix K to Part 50 – ECCS Evaluation models.

NUREG-1061, Vol. 3, concerning use of the leak-before-break approach, and a change in the Code of Federal Regulations 10 CFR Part 50[376] to include: "However, dynamic effects associated with postulated pipe ruptures [...] may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping". This possibility was not adopted in France, partly due to the uncertainties inherent to this approach[377].

Regarding the first confinement barrier, the U.S. NRC defined criteria (10 CFR 50.46, Appendix K) based on the state of knowledge in the 1970s on non-irradiated or slightly irradiated cladding material (Zircaloy-4). These criteria aim to satisfy the requirements for maintaining the core cooling capacity and a residual ductility of the fuel rod cladding at the end of a transient and to limit the amount of hydrogen produced to manage the risk of explosion in the containment. The criteria were formulated as follows:

– the cladding temperature must not exceed 2200°F (1204°C);

– the cladding oxidation rate during the transient or ECR (Equivalent Cladding Reacted) must not exceed 17% of the cladding thickness;

– the total quantity of hydrogen created by cladding oxidation must not exceed 1% of the quantity that would result from oxidation of the total cladding mass;

– changes to core geometry[378] must not prevent core cooling;

– the long-term removal of heat from the core must be ensured in all circumstances.

In a loss-of-coolant accident, the core cooling capacity depends not only on the ability of engineered safety systems to inject enough water to cool the fuel (thermal-hydraulic aspect), but also on the functional behaviour of the vessel internals and fuel assemblies under accident conditions (mechanical aspect).

As mentioned above, while thermal-hydraulic studies were conducted for all break sizes (up to the 2A break) and all possible break locations in the 900 MWe, 1300 MWe and 1450 MWe reactors, mechanical analyses were only conducted for 'conventional breaks with limited displacements'. These breaks are situated at specific locations based on the mechanical design of the pipes (welds, elbows, nozzles). Pipe size depends on the presence of anti-whip restraints. The time considered for a break to open is an important assumption in mechanical studies. From the outset of plant unit design in the French NPP fleet, it has been conventionally set to one millisecond.

[376] Appendix A, General Design Criteria 4.

[377] In particular, the uncertainty that affects models for determining a leak rate from the (assumed) dimensions of a through-wall defect. As indicated at the beginning of this chapter, for the EPR, the designer chose to use the pipe break exclusion principle, which is more comprehensive and based on high-level prevention of loss-of-integrity in the systems to which the principle is applied (only the main primary system and the main secondary system).

[378] This involves clad ballooning due to internal pressure in the fuel rods.

From the beginning of pressurized water reactor design, LOCA studies have also used conservative assumptions, in accordance with the design rules for design-basis (or reference) operating conditions and based on a deterministic computational method. This method uses realistic scientific simulation software[379] and 'penalizes' dominant parameters.

9.2.2. Fuel assemblies and fuel rods, vessel internals, reactor coolant system components

The criteria applicable to the first confinement barrier (fuel rod cladding), taken from US regulation 10 CFR 50.46, Appendix K, were given in Section 9.2.1.

Since the time when the calculation assumptions and technical acceptance criteria mentioned above were first defined, the operating conditions of reactors and the fuels they use have changed, leading to increased burnup rates, new fuel rod cladding materials, and more stringent fuel management principles. In addition, fuel behaviour in LOCA conditions has been studied in many R&D programmes conducted by operators and research institutes, including IRSN, and this research is ongoing. These programmes have led to better fuel characterization in LOCA conditions, particularly with regard to the relocation of fuel entrained by clad ballooning and bursting, as well as the ability of cladding to withstand the stresses applied during and after the accident. For strongly irradiated fuels, in certain conditions the dispersion of fuel particles out of the rod after it bursts (fuel dispersion) has been observed. The results of these numerous experiments are improving the ability of software models to simulate LOCA transients.

Since the 2000s, the U.S. NRC has been conducting a major overhaul of its regulations, in particular a revision of criteria relevant to the cladding temperature and oxidation rate in a LOCA situation. This process has not yet been completed.

In France, as noted in the introduction to this chapter, the question has been raised as to the relevance of changing the baseline for the study of LOCAs used in the design of pressurized water reactors, including the EPR (Flamanville 3). The various changes proposed by EDF were reviewed twice by the Advisory Committee for Reactors, in 2010 and then in 2014. This new baseline was applied for the first time as part of the safety reassessment studies associated with the fourth ten-yearly outage of the 900 MWe units. The main changes it introduces are presented in the following sections.

9.2.2.1. Mechanical strength of vessel internals, fuel assembly structures and reactor coolant system components

The safety demonstration pertaining to the mechanical strength of vessel internals – which support the core and convey the coolant – and the mechanical strength of fuel assemblies is based on mechanical studies that aim to achieve insertion of neutron-absorbing rods in the core and maintain fuel rod bundle geometry so

[379] Simulation software is considered realistic when it aims to reproduce as faithfully as possible the physical phenomena involved in the transient studied.

that it is capable of removing decay heat. It is therefore necessary to demonstrate that:

- hydraulic forces on the vessel internals do not compromise the stability, integrity, or function of these structures;
- hydraulic forces on the fuel assemblies, especially on the grids, do not compromise their functional behaviour under accident conditions. This involves demonstrating the buckling strength of the grids, which is necessary for a conventional situation in which LOCA effects are combined with earthquake loading.

The criteria to be used for mechanical strength analyses are the RCC-M criteria. In addition, concerning the functional requirements for the core cooling capacity and dropping the neutron-absorbing rods, there are maximum deformation limits for the relevant components and, for the fuel assembly structures, a lateral force limit that must not exceed the buckling limit of the irradiated grids.

The demonstration of how core cooling capacity is maintained by fluid circulation in the reactor coolant system also requires studying the behaviour of other reactor coolant system components (pumps, pressurizer, steam generators). For steam generators, the integrity of the tube bundle and that of the channel-head divider plate subjected to decompression loads must be studied for the large-break LOCA. The demonstration must show that the postulated rupture cannot make the accident worse and thus lead to greater risk for core cooling. Similarly, for the reactor coolant pumps, the acceleration of fluid as it flows towards the break may cause rotor overspeed. This must remain limited to avoid loss of integrity on the flywheel.

As indicated in the introduction to this chapter, in the new French baseline for the study of LOCAs, the same break spectrum is now used for both thermal-hydraulic and mechanical studies. This spectrum corresponds to conventional guillotine breaks with limited displacements and a longitudinal break, the maximum size of which is estimated using mechanical models. In addition, the break opening time is derived from a calculation of opening dynamics that take into account the stiffness of the reactor coolant loop and the presence of anti-whip restraints on the loop. To increase the break size, conditions in an extended operating cycle are considered because they are more conservative due to increased play between the components and the associated anti-whip restraints. The effects of ageing are also considered in the assessment of dynamic response in the relevant structures.

However, as part of the new LOCA baseline, studies are being conducted with realistic assumptions for the double-ended guillotine break of a reactor coolant system pipe, in the context of a 'robustness analysis'[380].

[380] This implicitly assumes failure of the anti-whip restraints.

9.2.2.2. Fuel behaviour

During the 2000s, the French baseline for the study of LOCAs diverged from the original US baseline, the fuel criteria of which were described above. The initial safety requirement stipulated that it was necessary to maintain residual cladding ductility up to the end of the transient, demonstrated by crush tests on ring-shaped specimens. This requirement changed, placing the focus on cladding quench resistance, demonstrated by tests conducted on cladding sections oxidized at high temperature that undergo (cold) thermal shock from quenching. This change did not affect the original criteria for maximum cladding temperature and maximum oxidation rate. However, the oxidation rate is now calculated by adding oxidation from normal reactor operation to transient oxidation due to the accident.

Having gained improved knowledge of fuel behaviour during a LOCA, the new baseline stipulates, as mentioned above, that structural cladding must withstand quenching combined with application of an axial force, as proven in integral testing that simulates an entire LOCA transient. EDF adopted a new safety criterion for the transient oxidation rate that varies as a function of the cladding hydrogen content at the time of the accident. The criterion of 1204°C for the maximum cladding temperature remains unchanged.

In addition, the fact that clad ballooning and bursting as well as fuel relocation have negative effects on the maximum cladding temperatures is now to be taken into account in the safety demonstration. In 2014, in view of the new safety reassessment studies associated with the fourth ten-yearly outage of the 900 MWe units, EDF proposed a new LOCA study method to take into account changing knowledge in fuel behaviour. There are several major changes in this new method compared to the deterministic method used previously, including for the EPR (Flamanville 3). First of all, EDF proposed statistical processing of the input parameters associated with the initial conditions and limit conditions, and of the parameters from the physical models of the CATHARE software (presented in Chapter 40). In addition, vessel modelling using the CATHARE software underwent changes, becoming a multidimensional model to better simulate the flows in the core and the annular space around the vessel. Finally, specific physical models were introduced in this software to consider the physical phenomena related to fuel behaviour, previously not modelled or poorly modelled, such as clad ballooning and bursting and its consequences in terms of hydraulic channel clogging and contact between the rods, and fuel relocation in the event of clad bursting.

The studies provided by EDF as part of the fourth periodic review of the 900 MWe units showed a possible activation of the postulated mechanisms mentioned above, which could ultimately compromise compliance with the 1204°C criterion (criterion involving only the risks of quenching rods embrittled by high-temperature oxidation when water arrives from the SIS). EDF is planning equipment and operating modifications that make it possible to avoid this risk of activating the postulated mechanisms (lowering the initial internal pressure in the rods, lowering the SIS accumulator filling pressure, partial restriction of the operating domain, etc.).

Finally, given the fuel management characteristics currently used in operating reactors in France and the maximum authorized burnup rates (covered in Chapter 28), in 2014 EDF provided information showing that the risk of fuel dispersion after clad burst could be excluded.

9.2.3. Reactor containment and equipment located inside

The loss-of-coolant accident is an operating condition to be considered for the pressures and temperatures that can be reached in the containment. The study of the accident pressures and temperatures in the containment determine:

- the bounding pressure conditions affecting the containment;
- the bounding pressure and temperature conditions affecting equipment that must be available in post-accident situations ('K1' profile – see Section 7.4.3);
- maximum water temperature in the sumps for designing the SIS and CSS engineered safety systems.

Even though the same accident is considered, certain specific assumptions differ from those used above, with the effect of maximizing the consequences for the containment.

In the case of the EPR (Flamanville 3), the breaks corresponding to nozzle rupture are taken into account to establish the long-term ambient conditions that the equipment in the containment must be capable of withstanding.

Chapter 10
A Special Issue: Steam Generator Tubes

As indicated in Section 6.3, the three successive confinement barriers between the environment and the radioactive products from fuel fission within the core of a pressurized water reactor include a very important and singular point: the steam generator tubes. They are part of the reactor coolant pressure boundary because the core cooling water circulates through them.

Here, the third barrier between the reactor coolant pressure boundary and the environment is thus not the containment, but the shells of the secondary system lines, which are very large because they contain the steam headers (at the outlet of the steam generators) and, downstream, even the turbines of the turbine generator. However, it can be assumed that if a problem occurs (tube leak, break, etc.), the secondary system is limited to the parts located between the steam generators and the main steam stop valves on each line.

The pressure shells of these secondary lines are protected against any overpressure by safety valves that release fluid directly to the atmosphere (see Figure 10.1). The secondary lines also have a system providing a main steam bypass to the atmosphere (MSBa), equipped with control valves. The opening threshold of these valves is set 5 to 10 bars below the opening threshold of the safety valves (depending on the type of reactor). This system is useful when the turbine or its condenser (MSBc system) is suddenly unavailable. The energy present and the residual heat are then removed by the release of steam to the atmosphere. It is also used during reactor startup, by actuating the control valves, when the power produced is insufficient to supply the turbine.

Given the volume of steam released on these occasions, the operator has not considered discharging into closed vessels.

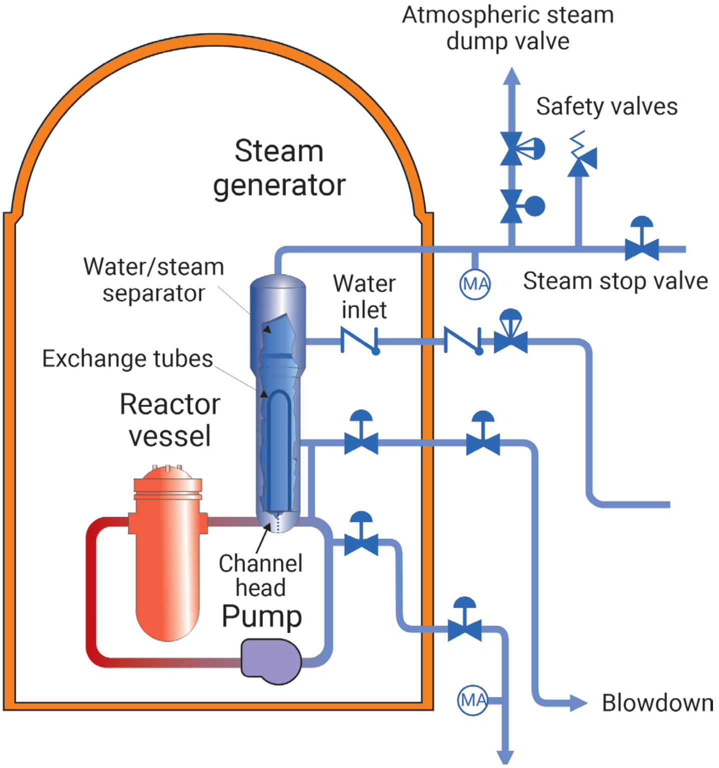


Figure 10.1. Discharge and safety valves on the steam lines (MA indicates monitoring of activity in the fluid). Georges Goué/IRSN.

The 900 MWe and 1300 MWe reactors are equipped with one MSBa line per steam generator. N4 reactors are equipped with two MSBa lines per steam generator. The EPR is equipped with one atmospheric steam dump valve (equivalent to MSBa) per steam generator.

Since the reactor coolant system is at a pressure of 155 bars in normal operating conditions, a sufficiently large break affecting one of the steam generator tubes is enough for the transfers of water and pressure to cause the discharge valves and safety valves to open on the affected secondary line. At that point, there is no longer any 'barrier' between the reactor coolant and the environment.

The steam generator tubes, with a total surface area of more than 15,000 m^2 per reactor and a wall thickness of only about 1 mm, are thus the sole constituents of the second and third confinement barriers as they are generally described. As a result, there are only two confinement barriers here.

Steam generator tube rupture (SGTR) was taken into consideration in the design of French pressurized water reactors, and the list of operating conditions for the first units classified this accident in the Category 4 operating conditions, with an estimated rupture frequency less than or equal to 10^{-4} per year and per reactor.

However, experience from around the world included damage and incidents that did not support this classification. Many causes of damage to steam generator tubes had been identified throughout more than forty years of operation, such as cracking due to stress corrosion, vibrational instability, loose parts, residual manufacturing stresses, etc. Table 10.1 shows the main ruptures or significant leaks in steam generator tubes observed in pressurized water reactors that are similar to French reactors[381]. All these leaks and ruptures only led to extremely limited consequences in the environment of the impacted nuclear power plants.

By 1993 (date of the Palo Verde 2 incident), this type of reactor had a cumulative experience of around 2500 years of operation in the world. The observed frequency of significant leaks was thus approximately 4×10^{-3} per unit and per year, distinctly higher than the maximum frequency chosen for initiating events belonging to Category 4 operating conditions.

Reclassification of the steam generator tube rupture accident as a Category 3 operating condition was a modification introduced in the list of operating conditions used for reactor design in the standard 1450 MWe (N4) series. This reclassification is not without consequences for the operator. The higher the probability of an accident, the more the tolerable radiological consequences must be limited, which may involve applying stricter operating requirements and improving plant unit technology.

Table 10.1. Main steam generator tube leaks and ruptures.

Country	Unit	Power	Date of event	Maximum leak rate in m^3/h
USA	Point Beach 1	500 MWe	26/02/1975	30
USA	Surry 2	800 MWe	15/09/1976	75
Belgium	Doel 2	400 MWe	25/07/1979	35
USA	Prairie Island 1	500 MWe	02/10/1979	90
USA	Ginna 1	500 MWe	25/01/1982	175
USA	North Anna 1	940 MWe	15/07/1987	145
USA	North Anna 1	940 MWe	25/02/1989	15
USA	Mac Guire 1	1200 MWe	07/03/1989	120
Japan	Mihama 2	470 MWe	09/02/1991	155
USA	Palo Verde 2	1300 MWe	14/03/1993	80

[381] Another noteworthy leak affected a steam generator tube at San Onofre 3 (1180 MWe) in the USA in 2012, but at a significantly lower flow rate (10 L/h). It highlighted problems in steam generator manufacturing that ultimately led to the definitive shutdown of this reactor.

Country	Unit	Power	Date of event	Maximum leak rate in m^3/h
Belgium	Tihange 3	1054 MWe	02/07/1996	40
USA	Indian Point 2	1000 MWe	15/02/2000	34
South Korea	Ulchin 4	1000 MWe	05/04/2002	30

In addition, the Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN) considered that it was necessary to continue to classify an SGTR bounding accident as a Category 4 event, under the assumption that a triggered safety valve on the relevant steam generator could remain jammed in the open position[382]. Électricité de France (EDF) took this request into account for 900 MWe and 1300 MWe reactors. For the more recent N4 series reactors and the EPR, given the two MSBa lines for the N4 series and the design of the safety injection system and the steam generator emergency feedwater system (EFWS) for the EPR[383], the rupture of two steam generator tubes was retained as an initiating event of a Category 4 accident situation.

Although no significant leaks or steam generator tube ruptures have been observed in the French fleet of nuclear power plants, the defects seen in these tubes and the impossibility of totally eliminating the risk of loose parts rule out concluding that, in theory, the situation is more favourable than the experience feedback from around the world.

The study of SGTR scenarios is presented in the following sections. It aims to show that by following the appropriate operating procedure, it is possible to cancel out the leak (by achieving a pressure balance between the primary and secondary systems) in order to reduce release to the atmosphere as much as possible.

10.1. Steam generator tube rupture as a Category 3 event

It is useful to briefly describe the sequence of events that would occur in a complete steam generator tube rupture[384] if the operators were to leave the facility only under the control of the automatic control systems. This description, related to a 900 MWe

[382] In the 1990s, tests showed that this type of safety valve was sensitive to the state of the fluid passing through it (steam or water). These tests highlighted the limits of using these valves which, due to their design, are only stable in operation when the fluid flowing through them is close to saturation.

[383] Since there are two MSBa lines on the N4 series reactors, one MSBa line is assumed to always operate in the event of an SGTR, which prevents the risk of triggering the secondary system safety valves. For the EPR, systems have been designed to prevent the affected steam generator from filling with water and the secondary system safety valves from being triggered. In particular, for the design of the safety injection system, a discharge pressure lower than the secondary system safety valve opening pressure was used (see Section 10.3.2).

[384] A double-ended guillotine break.

unit, is conservative to the extent that the design of these reactors is old and less robust in this type of accident compared to more recent plant series.

▶ Phase before human intervention

At the starting point, the reactor is assumed to be operating at 100% of its nominal power. Given the pressure difference between the reactor coolant system and the secondary system, the complete rupture of a steam generator tube leads to the transfer of 45 kg of reactor coolant water per second to the secondary system at the beginning of the transient.

This water is more or less contaminated by radioactive fission products released in the reactor coolant water through leaktightness defects in the fuel cladding (in addition to nitrogen-16 produced through neutron radiation of oxygen in the water).

In the reactor coolant system, the pressure drops, leading first to reactor trip and turbine trip, triggered by a 'pressure low' signal in the reactor coolant system at 130 bars. Next, the pressure drops below 120 bars, leading to automatic startup of the safety injection system and the emergency feedwater system (EFWS).

In parallel, the pressure in all steam generators increases rapidly up to about 71 bars, the minimum opening pressure of the atmospheric steam dump valves. Pressure is then stabilized by discharging steam to the atmosphere.

The safety injection flow rate and the flow rate of water leaving via the break naturally balance out, reaching an 'operating point' where the safety injection of water compensates for the water lost through the break. The water flow rate is then 25 kg per second (90 m^3/h).

In less than half an hour, the steam generator, followed by its steam line, fills with water. The atmospheric steam dump valves now release liquid water instead of steam, which increases the radiological consequences in the environment due to the greater retention of radioactive products in liquid water.

Since the fuel assemblies are correctly cooled during this phase (the core remains covered), there is no cladding rupture and the water from the reactor coolant system gradually released in the environment remains at the initial contamination rate of the water in the reactor coolant system before the accident.

If the situation were to continue without human intervention, all of the water in the tank used for safety injection would be transferred to the reactor coolant system, then the secondary system, then the environment. Unlike the case of a break in the reactor coolant system, the water lost via the break does not go into the containment sumps and thus cannot be reinjected in the reactor coolant system.

Eventually, in the absence of water makeup in the reactor coolant system, the fuel assemblies would be uncovered after about 20 h, causing rupture of the fuel rod cladding and transfer of volatile fission products to the environment, a situation with consequences that are obviously much more severe.

▶ Action taken by operators

To avoid this situation, operators must intervene to isolate the affected steam generator (by shutting down its EFWS) and decrease pressure in the reactor coolant system, starting by shutting down the safety injection system (which was maintaining a balance between the pressure in the reactor coolant system and the break). Once the EFWS has been isolated and pressure in the reactor coolant system becomes equal to or less than the opening pressure of the MSBa atmospheric steam dump valve of the affected steam generator, this valve can close, so that there is no longer transfer of water or release of radioactive products to the atmosphere.

The incident and accident operating procedures were developed to optimize the operators' handling of the SGTR accident. They are available in the control room and operators are specifically trained to perform them during this accident. For the SGTR scenario presented, the operator 'enters' the incident-accident operating procedures following reactor trip. The operator first reads the Diagnostics and Stabilization Document for the purposes of performing diagnostics on the state of the reactor and adopting a suitable strategy. In the case of an SGTR, detection of radiological activity in a steam generator leads to a procedure called ECP3, used for handling this type of accident (see Chapter 33 for information on the 'state-oriented' approach).

Procedure ECP3 aims to limit the transfer of water from the reactor coolant system to the secondary system, notably by stopping safety injection, followed by a sufficiently rapid decrease in the reactor coolant system pressure so as to bring it to the level of pressure in the affected steam generator. The required procedure also limits the rise in the water level of the affected steam generator by means of the blowdown system (SGBS). The primary objective of the procedure is to avoid opening a safety valve if it would lead to release of liquid water directly to the environment. This is due to the fact that the rate of rejection of reclosure of a safety valve becomes high when this valve, designed to release steam, is subjected to liquid water.

10.2. Preventing an SGTR accident, risk of multiple ruptures

While no significant steam generator tube rupture or leak has occurred in units belonging to the French nuclear power plant fleet, it is clear that, to avoid this type of accident, the programme of periodic non-destructive examination of the tubes is particularly important, even though it may prolong unit outage time and contribute to exposing workers to radiation. In certain cases, the defects observed in the tubes lead to preventively blocking them. The various types of defects observed in France are presented in Chapter 26.

It should be noted that the risk of a tube rupture spreading to one or more neighbouring tubes, already weakened, must not be overlooked. Parametric studies have been conducted to understand facility behaviour when an increasing number of ruptures occur, taking various additional failures into account. Beyond the rupture of

5 to 10 tubes, the overall kinetics undergo little change because the speed of water transfer is limited by the relationship between the safety injection flow rate and the capacity of the secondary line discharge valves. This maintains the entire system at the opening pressure of the atmospheric steam dump valves (71 bars for 900 MWe reactors). In the case of multiple ruptures of steam generator tubes, the procedure remains the same, with the objective of balancing pressure between the reactor coolant system and the affected steam generator.

To reduce the risk of steam generator tube rupture (and avoid an excessive loss of efficiency by blocking more than 15% of the steam generator tubes), it is possible to totally change the steam generators of a unit (see Figure 10.2).

In 1990, for the first time in a French reactor, the three steam generators in Unit 1 of the Dampierre-en-Burly nuclear power plant were changed. This first replacement in a French reactor also made it possible to better plan the same operation on other units. In 2019, steam generators were replaced in twenty-eight of the thirty-four 900 MWe units, and steam generator replacement operations began in 2017 on the 1300 MWe units[385].

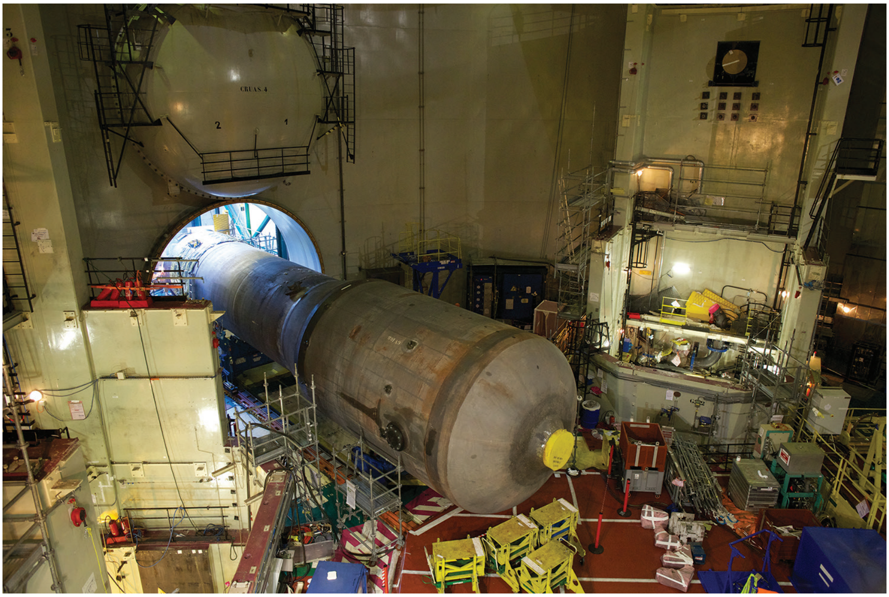


Figure 10.2. Steam generator replacement: steam generator passed through the equipment hatch. Jean-Marie Huron/Signatures/IRSN Media Library.

Prevention also involves detecting any leaks on steam generator tubes, even very small leaks. The detection systems were improved so that operators could make an early diagnosis and thus limit the possible progression of these leaks. In particular, and when

[385] It should be noted that these were not identical replacements (materials were changed along with other operations).

nuclear flux is significant enough, this involves detection of nitrogen-16, an element with a very short radioactive half-life (about 7 s), which is produced in the reactor coolant water when it passes through the core by the capture of a neutron by oxygen-16 and the emission of a proton. Any detection of nitrogen-16 in the secondary system water is thus indicative of a leak from the reactor coolant system to the secondary system. Due to the high energy of the gamma radiation characteristic of nitrogen-16 disintegration (10.4 MeV), detection can be continuous through the pipes of the secondary system. The detected activity is expressed directly in litres per hour on the indicators in the control room. If a leak rate is detected, the operators refer to the 'low-leak' operating rule ('R3F'), which allows continued unit operation only for very low leak rates, provided operating constraints are set up that are proportional to the leak rate and monitoring measures are reinforced if the flow rate exceeds a threshold or changes over time. For larger leaks, unit shutdown is required in a time frame that depends on the leak rate. Operators can be guided directly to incident or accident procedures.

In 2006, the application of 'R3F' to Unit 4 of the Cruas nuclear power plant led to rapid detection of a leak (about 0.5 m^3/h). The reactor was shut down by the operators, with no significant release.

10.3. Steam generator tube rupture(s) studied as a Category 4 event

10.3.1. 900 MWe and 1300 MWe reactors

The 900 MWe and 1300 MWe reactors are equipped with only one MSBa line per steam generator. A failure in the atmospheric steam dump system (failure to open upon triggering) would cause the opening of the safety valves, set at a higher pressure (by around 5 to 10 bars). In the case of an SGTR, this opening could cause problems, since proper operation of the safety valves with liquid water is not guaranteed (due to a risk of non-reclosure). If this type of safety valve were to jam in the open position, as happened in 1982 at the Ginna nuclear power plant in the USA, the situation would be more serious because operators would have to manage a steam generator tube rupture with a non-isolatable leak of reactor coolant water to the atmosphere.

As mentioned above, for the 900 MWe and 1300 MWe reactors this is considered as a Category 4 condition. The only countermeasure in this situation is to depressurize the primary and secondary systems to 1 bar to cancel out the water transfer flow rate from the reactor coolant system to the secondary system, and the transfer flow rate from the secondary system to the atmosphere.

10.3.2. 1450 MWe reactors and EPR (Flamanville 3)

The 1450 MWe reactors (N4 series) are equipped with two MSBa lines in parallel for each steam generator. This design makes these reactors robust in the case of a single failure of an MSBa valve. In these conditions, even if an MSBa valve jams in closed position, the other valve can be used to limit the pressure of the steam generator affected by an SGTR. The safety valves of this steam generator are thus not triggered, preventing the risk of their jamming in open position. With the possibility of a safety valve jammed open excluded, the Category 4 condition adopted for the 1450 MWe reactors is a clean break of two steam generator tubes, which would lead to faster filling of the affected steam generator and thus a higher risk of release than for the Category 3 SGTR, in which only one tube is assumed to break.

The EPR was designed to be particularly robust with regard to an SGTR accident. The objective set during the design phase was that the SGTR should lead to no liquid release. Reaching this objective was made possible by cancelling out the sources that contribute to filling the steam generator affected by the break and increasing its pressure, namely the steam generator emergency feedwater system and the break itself. This was accomplished by taking the following measures:

– by setting a maximum discharge pressure for safety injection below the opening pressure set point applied for the atmospheric steam dump valves if a high water level is detected in a steam generator, and below the opening pressure of the secondary system safety valves;

– by not starting up the EFWS if there is sufficient water inventory in a steam generator, which limits the rise in water level in the affected steam generator.

In addition, the EPR was designed to manage an SGTR accident automatically, including reaching a pressure balance between the primary system and the secondary system, namely by setting up two automatic control measures:

– automatic partial cooling so that the reactor coolant system can be depressurized to reach the discharge range of the medium-head safety injection (MHSI) pumps,

– automatic isolation of the affected steam generator so that it can be kept isolated at a pressure higher than the maximum discharge pressure of the MHSI.

For the EPR, there is only one atmospheric steam dump line per steam generator. However, since triggering of a safety valve is ruled out, the PCC 4 condition adopted is a clean break of two steam generator tubes, as for the 1450 MWe reactors.

The results of the Category 4 SGTR studies show that liquid release to the environment is much lower for N4 series reactors than for the 900 MWe and 1300 MWe reactors (with triggering of a safety valve); for the EPR, liquid release is negligible.

However, while lowering the discharge pressure of the safety injection system for the EPR does indeed reduce release from an SGTR accident, it is not without consequences for other types of accidents such as loss-of-coolant accidents (LOCAs). The lower the maximum safety injection discharge pressure, the later the compensation of water loss via the break, thus increasing the risk of core uncovery. Therefore, optimization is sought.

10.4. Provisions to mitigate the radiological consequences of SGTR accidents

The radiological consequences of an SGTR accident depend on two parameters: the quantity of (radioactive) fluid released to the environment and the initial radiological activity of the water in the reactor coolant system.

Concerning release to the environment, human intervention is crucial (900 MWe, 1300 MWe and 1450 MWe reactors) for this type of accident, where it is necessary to rapidly depressurize the reactor coolant system using steam generators that are in good condition. The first step is to meet the criteria allowing shutdown of safety injection (which itself contributes to maintaining pressurization of the reactor coolant system). In a second step, operators must cancel out the pressure difference between the primary and secondary systems to cancel out the leak rate. To this end, operating personnel is specially trained in the procedures for this type of accident, with frequent refresher courses, so as to limit the risks of significant external release. But, beyond this human aspect, the potential jamming of the secondary system safety valves in open position is decisive in determining how the scenario will progress and what its consequences will be.

To limit consequences for the environment, release should pass through the atmospheric steam dump valves, which are qualified to operate with liquid water and can be isolated by a second valve in the event of failure of the main valve, and not by the safety valves, which are not qualified for water and cannot be isolated. Another solution aims to avoid water overflow[386] in the affected steam generator by cancelling out the filling sources as rapidly as possible (point examined below).

▶ 'SGTR4' action plan implemented by EDF for 1300 MWe units

As part of its work programme associated with the third ten-yearly outage of the 1300 MWe units, EDF adopted an action plan aimed at reducing the impact on humans and the environment of the Category 4 steam generator tube rupture accident ('SGTR 4'). This is the accident that leads to the highest radiological consequences among the accidents without core melt. Actions taken to avoid complete filling of the affected steam generator include:

- equipment changes: automatic isolation of the emergency feedwater system (EFWS) of the affected steam generator when the very-high water level threshold is reached in the steam generator (THNGV)[387], which requires producing a specific THNGV signal for each steam generator;
- procedure changes: prolonged rapid cooling of the reactor coolant system to more rapidly reach the shutdown criterion of medium-head safety injection (MHSI) by lowering the reclosure pressure threshold of the atmospheric

[386] Filling the steam generator results in releasing water through the safety valves.

[387] *Très haut niveau (d'eau) dans un générateur de vapeur*.

steam dump valves (MSBa) by approximately 25 bars. The earlier MHSI shutdown occurs, the earlier operators can start depressurizing the reactor coolant system, thereby decreasing the pressure difference between this system and the affected steam generator, with the end result of a near cancellation of the water flow rate exiting the break.

These actions are sufficiently effective to prevent the affected steam generator from overflowing[388] when the reactor is initially at low power. To take into account an initial state at full power, EDF added another equipment modification to its plan: complete, automatic isolation of the main (controlled) feedwater system (MFWS) for the steam generators in the event of loss of off-site power (LOOP). This change helps limit filling of the affected steam generator if the SGTR occurs at full power.

Based on simulations conducted by EDF, these changes reduce calculated liquid release to the atmosphere by a factor of 16.

As for the 900 MWe units, starting with their third ten-yearly outage, EDF began making equipment changes such as automatic isolation of the EFWS and automatic shutdown of the MFWS to slow filling of the affected steam generator. However, since these changes do not meet the requirements for qualification in an accident situation, they cannot be used in the safety studies. As a result, EDF is expected to take measures to significantly reduce release to the environment for 900 MWe units, as part of the safety reassessment associated with their fourth ten-yearly outage.

For 1450 MWe units, a change similar to what was adopted for the 1300 MWe units was made to the procedures, making it possible to divide water release in the event of an SGTR by a factor of two.

▶ Adjustment of reactor coolant radiochemical specifications

Another way of limiting the radiological consequences of an SGTR accident is by lowering the thresholds in the radiochemical specifications for reactor coolant or, in other terms, the maximum authorized activity in the reactor coolant system. The extent of radiological consequences following an SGTR accident depends not only on the extent of release (mostly in liquid phase, since the fission products in this phase are assumed to be entirely released to the atmosphere), but also on the degree of contamination in the reactor coolant system (which contaminates the secondary system via the break in the steam generator tube) by fission products and corrosion products. Once the SGTR was classified as a Category 3 condition, the thresholds of the radiochemical specifications changed drastically in 1987 (particularly the reactor shutdown threshold relevant to the iodine-131 equivalent[389]). The radiochemical specifications for reactor coolant then underwent successive changes. They became more stringent and new indicators were introduced, due to the occurrence of specific

[388] Once again, this involves filling the affected steam generator with water, which means that in the event of MSBa blockage, the safety valves are triggered by water.

[389] This indicator (^{131}I equivalent) is used to take into account the radiotoxicity of the various iodine isotopes.

problems. The indicators used to monitor radiological activity in the reactor coolant and the changes in the associated thresholds are presented in Section 28.1.

In 2009, EDF informed the French Nuclear Safety Authority (ASN) of its objective to extend the operating lifetime of in-service reactors beyond 40 years (see Section 30.5). In 2010, ASN considered that the safety reassessment studies for extending the operating lifetime of reactors in the nuclear power plant fleet should aim to reduce the radiological consequences of accidents as much as reasonably achievable, while striving to meet the safety objectives applicable to new reactors, such as those adopted for the EPR and those defined by WENRA for new reactors.

By 2018, EDF had indicated that it planned to reduce the shutdown threshold of the 900 MWe units for the iodine-131 equivalent in the reactor coolant system water during a power transient ('iodine peak')[390].

[390] Measure also proposed to ASN for 1300 MWe units.

Chapter 11
Providing for Hazards: General Considerations and Internal Hazards

11.1. General considerations on providing for hazards

The US licence that served as the basis for 900 MWe reactor design included protection of facilities against a certain number of internal projectiles (valve stems, sensor thermowells, shafts in control rod drive mechanisms) and also required making provisions for a characteristic earthquake on site. Ongoing discussions in both the USA and Europe regarding potential failures led to a gradual increase in protection against internal and external hazards. Hazards have never been studied in the same way as operating conditions, which were divided into categories of decreasing estimated frequency; the consequences of a particular hazard must, in every case, be small enough to be considered acceptable.

Certain phenomena or events can cause hostile conditions and can directly or indirectly cause equipment damage that affects the safety of a nuclear power reactor. They are referred to as 'hazards'. Depending on their origin[391], they are known as:

[391] Malicious acts are also hazards, but are not discussed in this document. See, for example, the document entitled A Comparative Approach to Nuclear Safety and Nuclear Security, J. Jalouneix et al., Reference Documents Series, IRSN/EDP Sciences, 2009.

- internal hazards when the source of the hazard is inside the facility; for example, a fire in a room, flooding following a tank rupture, the impact of a section of ruptured pipe on other equipment (a hazard caused by a phenomenon commonly referred to as 'pipe whip'), a load (such as a component during a handling procedure) being dropped on another component or system, etc.;
- external hazards of natural origin: for example, earthquakes, flooding from waterways, failure of an embankment or dam upstream of the facility, high or very high temperatures (heatwaves), strong winds, etc.;
- external hazards associated with human activity outside the facility, such as an accidental gas explosion near the facility.

As with the events discussed in the previous chapters, based on a defence-in-depth approach, measures are taken to prevent hazards, but their occurrence is still postulated and other measures are taken to mitigate them. However, design and operating measures can only have a very limited influence on the occurrence of an external hazard; this makes siting particularly important.

In view of the associated design rules and in spite of the direct or indirect effects of a hazard (see for example ASN Guide No. 22), it must not compromise the availability of any system, structure or component inside the nuclear reactor that performs a safety function, especially:

- control of reactivity (obviously including reactor shutdown[392]);
- heat removal (or residual heat removal if the reactor is shut down);
- confinement of radioactive substances.

In other words, a safe reactor state[393], in which the functions mentioned above can be assured in the long term, must be reached and maintained following a hazard.

For this purpose, any equipment that performs a safety function is protected against the effects of hazards:

- either by measures taken to prevent the effects of the hazard from reaching the equipment; this is the case, for example, for equipment protected by a safety net to protect it from the risk of projectile impacts in strong winds, or equipment protected by structures that can withstand falling loads, etc.;
- or by design, enabling the equipment to remain operational even if it is affected by the hazard; this is the case, for example, for equipment designed and sized to

[392] Generally speaking, the operator must be able to make a rapid assessment of the risks if an external hazard occurs, in order to keep the reactor(s) on the affected site in the shutdown state considered to be safest or to pursue their operation (RFS I.3.b).

[393] This concept is defined in the Focus feature in Chapter 8.

withstand the earthquake conditions incorporated in the reactor design basis, or even an extreme earthquake[394].

Generally, for reactor design and the safety demonstration, risks related to hazards are taken into account in two stages:

– determination of the characteristics of hazards likely to occur on each site: a reference level is defined for each hazard taken into account;

– implementation and demonstration of appropriate protection against each hazard identified in the above process.

For some hazards, (such as pipe ruptures or internal projectiles), geographical separation of equipment important for safety can be one way of protecting redundant trains from the impact of a hazard. For other hazards, particularly external hazards of natural origin, special studies are often necessary because these hazards can have an effect on redundant trains, or even all the facilities on a site.

With regard to internal hazards, the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors (applied to the EPR) provide clarifications and further information on the subject in Section F.1.1 (General Requirements):

> "The possibilities of common-mode failures due to internal hazards can be minimized by the installation of the parts of the safety systems trains which are located outside the containment building in divisional areas designed so that even the complete loss of one divisional area due to a specific internal hazard would not prevent the fulfilment of the three fundamental safety functions, assuming the application of a single failure consistently with the safety demonstration rules applied for the reference transients, incidents and accidents[395]. Installation provisions for redundant equipment of safety systems not separated by the divisional arrangement have to be specified by the designer.
>
> Moreover, the safety demonstration has to be done for each internal hazard with the assumption that all the affected non-protected equipment is lost and with the consideration of an aggravating single failure and of first operator actions with the same rules as for the reference transients, incidents and accidents. In principle, internal hazards which do not result from such transients, incidents and accidents should not induce a plant condition which would be categorized as incident or accident. Otherwise, the designer has to show that this plant condition is covered, regarding its probability and consequences, by the assessment of the reference incidents, accidents and multiple failures conditions.

[394] Based on operating experience feedback from the Fukushima Daiichi nuclear power plant accident (see Section 6.8).

[395] These are the 'reference operating conditions' (PCC 2 to 4), according to the terminology used in the technical directives, recalled in the Focus feature in Chapter 8.

> Links between internal hazards (such as flooding resulting from pipe breaks or fires resulting from explosions) have to be considered in the safety demonstration as well as internal hazards which could result from external hazards or severe accidents [...]."

WENRA stated in its reference levels (in January 2007 and subsequent versions, Section 8.2) that "the worst single failure shall be assumed in the analyses of design-basis events" ('design-basis events' being a concept that, for WENRA, encompasses all types of hazards). ASN Guide No. 22, published in 2017, takes the same approach[396]. An aggravating failure is now taken into account in new hazard studies, particularly as part of the studies associated with the fourth ten-yearly outages of 900 MWe units.

The design of systems used for protection against hazards usually follows an approach based on defining and taking into account 'load cases'[397] in order to ensure that the equipment necessary to perform safety functions is designed and sized to withstand the hazard and therefore remain available.

As a complement to this approach, analysis may consider the hazard as an event: it examines the effect of the hazard on the facility as a whole and ensures that equipment that is not protected or not designed to withstand the hazard is not likely to cause unavailability of equipment that must remain available. In this manner, if equipment that is not considered important to safety falls during an earthquake, it must not damage equipment designed or protected to withstand an earthquake. This illustrates the 'earthquake as an event' concept, introduced in Section 8.4.3.

When the hazard can have 'functional' consequences such as loss of off-site power or loss of heat sink (due to clogging of water intakes, etc.), taking an event-oriented approach of this kind makes it possible to verify the availability of the equipment necessary to manage this type of situation in the hazard conditions in question.

Finally, all the initial states of a reactor should be considered in the study of hazards, especially the shutdown states, in the same way as for the study on design-basis (or reference) operating conditions (see Section 8.4.1 on this subject)[398].

The way internal hazards are taken into account in the design of pressurized water reactors is discussed in more detail in the rest of this chapter.

11.2. Potential projectiles inside the containment

All equipment or parts of equipment that could, as a result of a failure, be thrown or projected through space, are considered to be potential projectiles. Internal projectiles in the nuclear island could be parts of pressure equipment, rotating machinery,

[396] Sections 3.3.2.3.1 and 3.3.3.3.1 of the guide.

[397] In principle, the approach that uses the 'load case' – an expression that comes from design and construction code practice – is general in nature and can be used both for internal hazards, such as pipe whip, falling objects or projectile impacts, and for external hazards (such as earthquakes).

[398] ASN Guide No. 22 states that non-plausible combinations of internal or external hazards may be disregarded, given appropriate substantiation.

or items emitted on a secondary basis in reaction to a projectile impact. The case of heavy objects dropped during handling is also examined. Projectiles that are pipes are excluded, since the conditions and effects of pipe breaks are analysed separately; both subjects are discussed later on (sections 11.3 and 11.8).

Protection against internal projectiles in the nuclear island is defined such that the emission of a projectile:

- does not compromise availability of the safety functions;
- if it leads directly to a loss-of-coolant accident:
    - the projectile must not cause a loss of leaktightness of the third confinement barrier,
    - it must not cause a secondary fluid leak,
- if it leads directly to a loss of secondary fluid, it must not cause a loss of reactor coolant.

To minimize the risks of common-mode failures on systems required to achieve and maintain a safe reactor state, construction measures are taken. All equipment capable of producing projectiles is installed and oriented such that any projectiles that could be envisaged are, as far as possible, quickly stopped by a civil works structure. Moreover, as part of the approach to managing risks from projectiles, it is considered that projectiles for which the probability of impact on the sensitive parts of a reactor (such as equipment important to safety) is low should not be considered concomitantly with other independent events with a low probability of occurrence, such as an earthquake or a reactor-coolant-system pipe break.

To illustrate this approach, the following components are considered to be potential projectiles inside the containment:

- the air bleed plugs at the top of the control rod drive mechanisms,
- the control rod drive shafts,
- the caps, servomotors or stems of certain valves,
- temperature probes and pressure taps,
- pressurizer heaters.

The possible projectile trajectories are studied and it must be verified that a suitable ‘barrier’ will interrupt each trajectory before the projectile hits any sensitive equipment.

Ejection of the air bleed plug from a control rod drive mechanism is studied in the same way, but because it leads to a reactivity accident, it is studied as a Category 4 condition as regards its consequences for the core and the reactor coolant system.

Protection against the projectiles mentioned above consists of:

- projectile shields for the air bleed plugs at the top of the control rod drive mechanisms,
- 'bunkers' around the reactor coolant loops and steam generators as protection against other projectiles.

In contrast, reactor coolant pump flywheels are not considered to be potential projectiles because:

- the flywheel design and choice of materials make the risk of a fast fracture during normal operation extremely low;
- in the event of overspeed due to an accident, the speed that would cause the ductile failure of the flywheel under increased stress is greater than the maximum speed reached during the accident.

Periodic in-service monitoring of these flywheels is carried out to detect any incipient cracking in zones of irregular shapes, such as inside key slots. An incipient crack due to a defect can only occur during overspeed when the defect size is far greater than the detection threshold of the in-service inspection methods used.

11.3. Effects of pipe breaks

The general installation of systems must be designed to prevent an unforeseen initial incident or event from spreading or contributing to an accident with greater consequences than those of the initial incident.

Pipe ruptures or cracks are studied to determine construction measures that would mitigate their consequences, with two aims:

- protection of the equipment necessary to bring the reactor to a safe state and maintain that state, as well as limit the radiological consequences of the event;
- avoiding any aggravation of the initial incident or accident, i.e. no spreading, for example, from one part of a system line to another part of the same line, or from one line to another line that is important to safety.

Apart from the loss of function of the ruptured or cracked system line, the following consequences of a rupture or crack are also taken into account:

- the effects of the flow of fluid, which may be radioactive (jet, flood, irradiation and contamination),
- changes in local atmospheric conditions (pressure, temperature, humidity),
- dynamic effects of broken pipes: pipe whip (formation of a 'plastic swivel joint' at the first obstacle encountered by the pipe) and incidence on the operability of the active components supported by the pipe.

The following measures are taken when installing systems to mitigate the consequences of a rupture for neighbouring components:

- geographical separation (sufficient distance between components,
- otherwise, physical separation (concrete shells or walls),
- otherwise, the installation of anti-whip devices (metal frames, stops, pipe anchors, etc.).

In design studies, it is generally considered that:

- pipes containing or carrying a high-energy fluid (high-energy pipes, at an operating pressure greater than 20 bars or operating temperature greater than 100°C) may whip when they break;
- pipes containing or carrying a medium- or low-energy fluid (medium-energy pipes, at an operating pressure less than 20 bars or temperature less than 100°C) may crack, but must not whip;
- pipe whip on a pipe containing or carrying a high-energy fluid may break a pipe of the same type with a smaller nominal diameter, or cause a crack in a thinner pipe of the same or larger nominal diameter.

These principles were applied in the equipment design and layout drawings, starting from the first units built in the French nuclear power plant fleet. Very comprehensive verifications were then carried out on site on a 900 MWe unit and a 1300 MWe unit, after construction. The few residual problems identified during these checks were obviously corrected on all units.

11.4. Projectiles generated by a turbine rotor failure

For the units at Fessenheim, Bugey and the sites under the first programme contract (CP1) – Tricastin, Gravelines, Dampierre-en-Burly and Le Blayais – the turbine generator was located 'on a tangent' to the nuclear island.

It was during construction of the two Fessenheim units that a risk was identified whereby the reactor building or other buildings containing equipment important to safety could be struck by projectiles resulting from rupture of a large wheel in the turbine LP cylinder (in the turbine hall). This type of rupture should not be confused with the rupture of a few turbine blades, which is much more likely, but has no impact outside the turbine housing. The probability of a turbine burst was calculated to be 10^{-4} per turbine per year, by US studies covering the worldwide NPP fleet.

An accident of this kind can produce projectiles of different sizes and different energies. It has been estimated that, for the turbine generators at the 900 MWe units, the most dangerous missile that could be envisaged, because it has the greatest energy, would have a mass of 3.6 tonnes and an initial velocity of 92 m/s (i.e. a kinetic energy of approximately 15 MJ). A projectile like this would be emitted in a direction perpendicular, or almost perpendicular, to the rotation axis of the turbine and it could therefore strike sensitive parts of the facility. This is what was observed after two turbines burst at the conventional thermal power plants at Porcheville and Gennevilliers in France.

Walls or shields capable of absorbing that amount of energy were installed during construction in the Fessenheim units, between the turbine hall and the buildings requiring protection. Walls were directly integrated into the design of other facilities with tangential turbines.

Using the opportunity provided by other modifications to the turbine hall, EDF adopted a 'radial' layout for the turbine halls of the 900 MWe reactors under the second programme contract (Cruas-Meysse, Saint-Laurent-des-Eaux, Chinon). This layout removed the risk of a nuclear island being struck by a projectile emitted by the turbine of the same unit or its twin.

During the safety review of the 1300 MWe units at the Paluel nuclear power plant (which has four independent units with radial turbines), the problem arose of the possibility of units 3 and 4 on the site being struck by projectiles from the turbine generators of units 1 and 2, and vice versa.

The safety organizations examined the precautions taken by the operator to reduce the risks of turbine burst through ductile failure during overspeed or through brittle fracture. These precautions involve preventing overspeed by using appropriate devices, as well as manufacturing methods and in-service inspections to identify any faults and monitor their progression before they become critical.

Although appreciated, these measures were not considered sufficient to ignore statistics based on 70,000 turbine-years worldwide, which gave a burst probability of 10^{-4} per turbine per year. These statistics showed that 70% of ruptures occurred at nominal speed and 30% at overspeed.

Given the planned layout of the units, applying this value led to a 4.5×10^{-6} probability of unacceptable release of radioactivity per unit per year for bursting of a turbine generator. This value was considerably higher than the indicative value of 10^{-7} per year proposed by the USA (which alone would justify further study of this risk), and was already used at the time (1977) in France for certain external hazards.

The safety organizations then sought to assess the conservatism of this probability. The following points were observed, but it was not possible to assign them a value:

- the statistics used took into account all turbine bursts, regardless of the size or energy of the projectiles emitted;
- projectiles displaying energy that was less than or equal to that of a quarter of a turbine wheel emitted at nominal speed could be stopped by the walls of buildings, without taking any special measures;
- the most probable trajectories of the projectiles with the highest energy were largely perpendicular to the rotation axis of the turbine and they would therefore not reach buildings important to safety.

These observations led to the conclusion that:

- it was possible to position the four 1300 MWe units at Paluel in parallel and with little space between them, without additional protection being necessary;

– different building layouts were worth considering wherever the site characteristics allowed.

These considerations were then adopted for the construction of subsequent power plants. The measures adopted starting with the first 900 MWe units and up to Flamanville 3 are shown in Figure 11.1 (with a few variants, such as the fan arrangement of the pairs of units at the Cattenom nuclear power plant).

These principles were formalized in a fundamental safety rule in 1995 (RFS I.2.b).

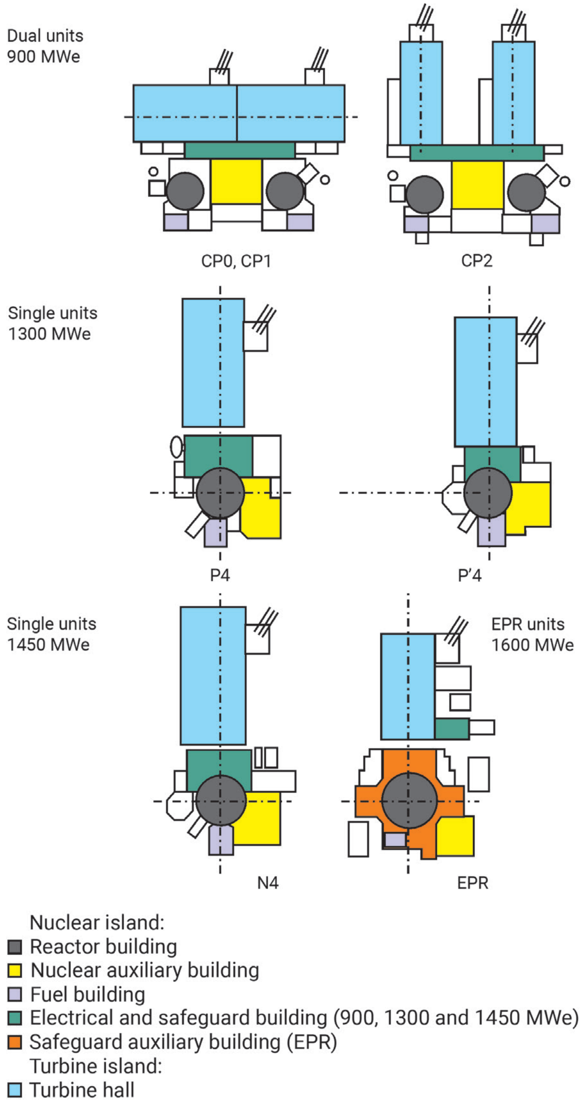


Figure 11.1. Layout of units and their turbine generators. Georges Goué/IRSN Media Library.

11.5. Protection against load drops

It was stated in Chapter 8 that a fuel assembly dropped during handling, causing loss of integrity of the cladding and the release of radioactive substances within the facility, was one of the design-basis or reference operating conditions.

The risk of dispersion of radioactive substances could also be associated with handling equipment other than fuel assemblies, but also containing nuclear materials or radioactive substances, at different locations in a nuclear power plant.

Handling objects in general could be a source of risks associated with the consequences of falling loads or collisions with other equipment or structures that are important to safety (protection systems, engineered safety features, spent fuel assemblies, etc. on the ground or at height).

There is a major risk associated with the transport packaging of spent fuel outside the unit, because the packaging is particularly heavy (1100 kN) due to the necessary protection measures.

Personnel and equipment need to be protected against the risks of falling loads at most industrial facilities. This risk also exists at a nuclear facility, and it must be addressed. However, that is not what will be discussed here. The text that follows will focus mainly on the risks of dispersing radioactive substances or risks due to handling incidents or accidents that could entail significant exposure. To remain consistent with principles applied regarding other sources of radioactive dispersion, the reliability of lifting equipment could be subject to much more stringent requirements and design precautions than those applied for 'conventional' occupational safety purposes.

Some load drops, however, especially of heavy loads, can be ruled out if a high level of prevention is demonstrated, especially by reliability studies on the relevant lifting equipment[399].

11.5.1. Risks related to spent fuel transport packaging

Spent fuel transport packaging is subject to international regulations[400] pertaining to transport on public highways.

Transport safety, like facility safety, is based on the defence-in-depth concept, which consists of implementing several levels of protection, both technical and organizational, to protect the public, workers and the environment in routine situations and in the event of incidents and accidents.

[399] This is particularly the case for the circular overhead crane in the reactor building.

[400] Because spent fuel can be shipped across borders, regulations are based on international requirements. A committee of experts from the UN Economic and Social Council draws up the 'UN model regulations', which contain recommendations for the transport of hazardous goods. These goods are divided into nine classes based on the type of hazard; class 7 is radioactive material. The recommendations specific to radioactive material are contained in the IAEA SSR-6 document, which serves as the basis for European, and particularly French, regulations on the subject.

'Packages' (the packaging and the radioactive substances it contains) must[401]:

- provide protection from the ionizing radiation emitted by these substances, for example, by means of shielding that attenuates the radiation;
- prevent the release of these substances from the packages by means of an outer casing and a closure system that ensures the packages are leaktight;
- prevent a nuclear chain reaction from occurring if the contents of the package consist of fissile materials, particularly by limiting the contents and ensuring the package is leaktight (because water can contribute to starting a chain reaction – see Chapter 5);
- where necessary, provide protection against the risks associated with the release of heat by the contents, for example, by using cooling fins;
- where necessary, provide protection against the chemical risks posed by the contents.

Type B packages are used for transporting the most highly radioactive substances, such as spent fuel from nuclear power plants and vitrified high-level nuclear waste from the La Hague reprocessing plant.

In view of the high level of risk posed by type B packages and packages containing fissile materials, regulations require them to be tested in conditions simulating a severe accident:

- a drop test from 9 m on an unyielding target. The fact that the target is unyielding means that all the energy from the fall is absorbed by the package, a very penalizing constraint. If a heavy package falls while it is being transported, the ground will yield and absorb some of the energy. So a fall on an unyielding target from 9 m could correspond to a fall from a much greater height onto ground that does yield. This test can be used to simulate cases where the vehicle transporting the package hits an obstacle at a certain speed;
- a penetration test (see Figure 11.2): the package is dropped from a height of 1 m onto a metal punch bar. The aim is to simulate damage to the package by perforating objects (such as debris ripped off the vehicle in an accident);
- a fire test at 800°C for 30 min. This test simulates the fact that the vehicle could catch fire in an accident;
- an immersion test under 15 m of water for 8 h. This tests pressure resistance should the package fall into water (into a river beside the road or into a port when a ship is being unloaded). Some type B packages must also undergo an advanced immersion test (under 200 m of water for 1 h).

In view of these requirements, the risk of the contents leaking from a spent fuel transport package can be considered as ruled out.

[401] See the ASN website on this subject.

The design of French facilities also strictly limits the areas in which these packages must be moved. They must not enter the reactor building. In the fuel building, their path of movement is strictly limited by mechanical arrangements to ensure they are never above the spent fuel storage area.

The crane that transports packages must be capable of withstanding the seismic margin earthquake and demonstrate high reliability. It is nevertheless envisaged that packages may be dropped and measures are taken to ensure that this does not have any consequences for facility safety.

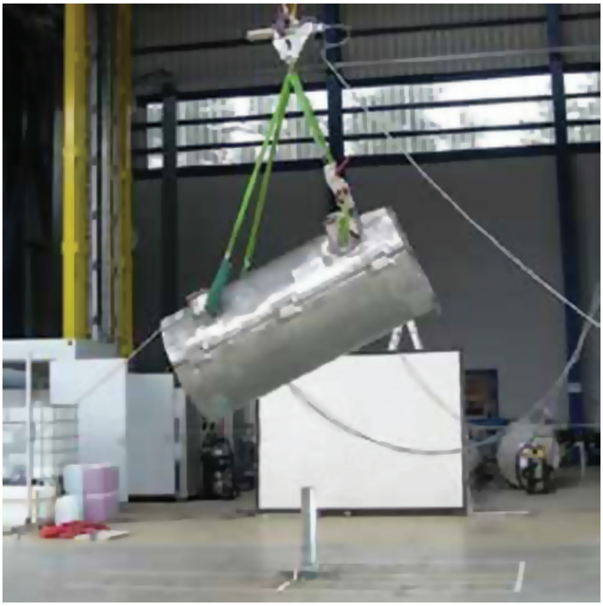


Figure 11.2. Drop test on a (vertical) punch bar of a Daher-NCS DN30 package model (type B package). ASN.

The risk associated with this event is a loss of leaktightness of the spent fuel pool, which can lead to loss of water from the pool, uncovery and heating of the fuel and the release of radioactive substances in the fuel building. This would cause a high level of direct exposure in the building, but also on the site and in the surrounding area.

Package drops are studied in the handling opening and in the loading pit, vertically and diagonally; construction measures prevent the shock wave produced by a package drop from being transmitted to the spent fuel pool. The civil works that support the pool are isolated from civil works in the package handling area.

In the oldest reactors, where this isolation does not exist (CP0 type 900 MWe reactors), hydraulic or mechanical dampers have been added at the bottom of the loading pit and at the bottom of the handling opening (see Figure 11.3).

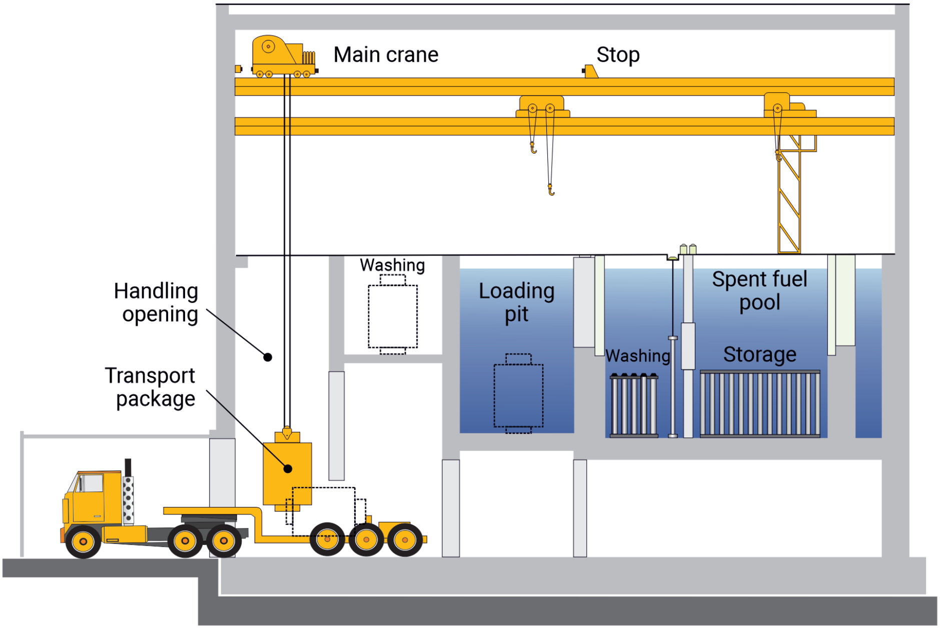


Figure 11.3. Handling a transport package in a 900 MWe reactor. Georges Goué/IRSN.

For later reactors, those in the P'4, N4 and EPR series, the drop risk has been excluded by implementing loading under the pit (see Figure 11.4). The transport package remains at site ground level. However, this solution introduces the possibility of water leaking from the bottom of the loading pit, which has therefore been designed accordingly.

11.5.2. Other handling risks

It should be emphasized that there are specific risks associated with handling the filters and resins[402] used in nuclear power plants, as well as risks arising from handling in general, where the items being handled are likely to pass over pipes or other equipment important to safety.

By giving particular attention to this aspect of safety, the risks can be satisfactorily identified and addressed.

[402] Ion exchange resins used to treat contaminated water.

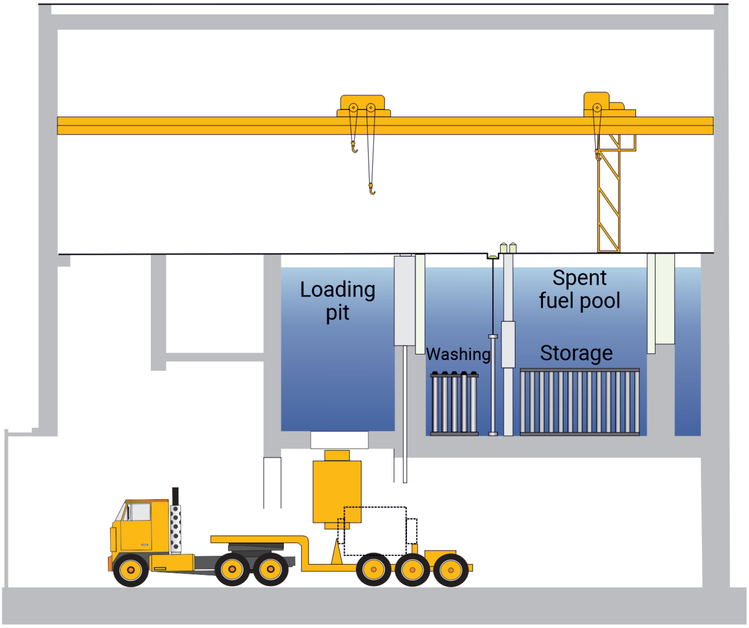


Figure 11.4. Loading under the pit (P'4, N4 and EPR reactors). Georges Goué/IRSN.

11.6. Fire protection

Fire is one of the most feared events at a nuclear power plant, particularly because of the significant probability, as at any industrial facility, of the outbreak of fire, as well as the potential severity of its consequences for facility safety.

The Design and Construction Rules for Nuclear Power Plants with PWRs – Fire Protection Rules (RCC-I), drawn up by EDF in the early 1980s, defined fire protection as all measures taken to prevent fire risks and mitigate the consequences. It specified that these measures should meet three objectives:

- ensure the safety of people,
- limit equipment damage that could lead to long-term unavailability,
- prevent compromising the availability of safety functions.

Although a fire with serious consequences for nuclear safety has never occurred at a French facility, despite around twenty fires being reported each year within the entire French nuclear power plant fleet, the event in 1975 at the Browns Ferry nuclear power plant in the USA (see the Focus feature below)[403] has not been forgotten. Because of

[403] A significant fire also occurred in 1989 at the Vandellos nuclear power plant (a gas-cooled reactor [GCR]) in Spain; this event is mentioned later because it led to major internal flooding.

the importance of the issue, the Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN) drew up a special fundamental safety rule, RFS V.2.j, released in 1988.

This document has been replaced, since the 2000s, by regulatory texts specifying in greater detail the requirements to be met by operators, particularly as regards internal hazards such as fire.

More recently, the French Nuclear Safety Authority (ASN) updated the regulations by preparing a decision[404] on the rules applicable to basic nuclear installations to mitigate the risks associated with fire. This decision was issued in 2014 and takes into account the proposals contained in a report by IRSN released in 2011[405].

#FOCUS

The fire in March 1975 at the Browns Ferry nuclear power plant in the USA

On the Browns Ferry site (Alabama), there were two 1100 MWe boiling water reactors in service and a third under construction at the time of the accident. The two units in service were operated from a joint control room. On 22 March 1975, a fire broke out in the cable spreading room, under the control room, at the point where the cables pass through a wall into the reactor building of Unit 1, which was at slight negative pressure. The original seals in the wall had been removed for the installation of extra cables. When the work was finished, the personnel were resealing the hole through which a group of 10 raceways passed, all trains combined, and were looking for the final leaks with a candle flame. The sealing material, which was highly flammable, caught fire. Drawn by the negative pressure, the fire spread into the reactor building, but the workers did not immediately realize this. The scale of the accident was only grasped once instrumentation and control cables for the two units had suffered significant damage, causing them to short circuit. Many of the systems for Unit 1 were thus knocked out of service. The operating personnel nevertheless managed to shut down the reactor, bringing it into a stable safe state. There were no releases or near-releases of radioactive substances.

The accident at the Fukushima Daiichi nuclear power plant in Japan on 11 March 2011 increased general awareness of the need to strengthen defence in depth and

[404] ASN Decision 2014-DC-0417 dated 28 January 2014.

[405] *Démarche d'analyse des risques d'incendies dans les installations nucléaires* (Analytical Approach to Fire Risk in Nuclear Facilities), IRSN, 20 July 2011.

reinforce the French safety approach to take into account situations that, until then, had been considered highly implausible, including certain combinations of situations, but that could simultaneously affect several facilities (see Section 6.8). This is the case in particular for fires that could result from a more dangerous hazard than the ones specified in the design basis for facilities.

The top-priority objective of fire protection at nuclear power plants nevertheless remains the same: avoid compromising availability of the safety functions. These functions are generally performed by redundant equipment, so that damage to a single item of equipment cannot lead to the loss of a safety function[406].

▶ Approach to studying fire-related risks

The control of fire[407] risks at nuclear power plants, as for other risks, is based on the implementation of successive levels of defence that are independent enough to achieve the lowest possible level of risk. In the case of fire, these different levels of defence must cover in particular:

- prevention of outbreaks of fire;
- detection and rapid extinguishing of outbreaks; the aim of this is, on the one hand, to keep outbreaks from developing into a full fire, and on the other, to restore normal operating conditions or, failing that, bring the reactor to a stable safe state;
- limiting any aggravation and spreading of fire that could not be kept under control in order to minimize its impact on nuclear safety and achieve a stable safe state.

The chemical reaction of combustion can only occur when the following three elements are present:

- combustible material,
- an oxidizing agent (usually oxygen in the air),
- energy for activation.

This principle is illustrated in what is known as the ‘fire triangle’, shown in Figure 11.5 below.

Preventing outbreaks of fire therefore relies mainly on limiting the amount of combustible materials present in the facility and managing potential sources of ignition, particularly during work with ‘hot spots’[408]. A risk assessment must be carried out for any introduction of fire loads not covered by the safety demonstration and, where necessary, compensatory measures must be taken.

[406] Fire protection also aims to ensure worker protection through application of the Labour Code, which obviously also applies to nuclear facilities.

[407] See the IRSN report published in 2011, mentioned above.

[408] Welding, for example.

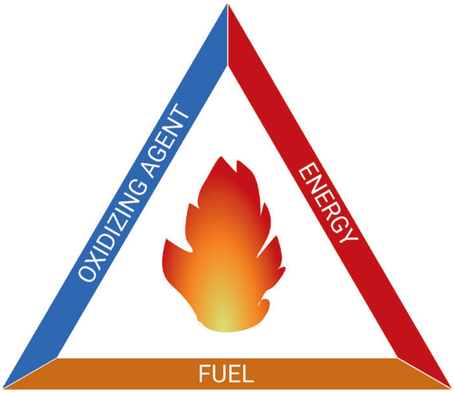


Figure 11.5. 'Fire triangle'. IRSN.

Detection and rapid extinguishing of outbreaks of fire rely on continuous facility monitoring using detection systems, fire response systems and firefighting resources. Firefighting resources can be supported by emergency response resources from outside the power plant. In some rooms, it may also be necessary to install automatic extinguishing systems to keep the damage caused by a fire to a minimum. Smoke extraction systems are also installed to allow response teams to intervene.

It is important to ensure that the chosen firefighting resources do not lead to other risks such as:

- internal flooding,
- electrocution, short circuits,
- suffocation of personnel,

both during normal use and in the event of inadvertent operation.

More generally, the planning of response procedures and access must take into account radiological considerations.

Limiting the spread of a fire is based mainly on dividing the facility into 'fire compartments' that can contain a fire through the installation of fire-resistant walls and doors as well as fire dampers. The boundaries of these fire compartments must be defined so as to limit the amount of equipment damaged in a fire. For example, redundant equipment is not normally placed in the same fire compartment; by default, it is protected or is separated sufficiently to prevent a common-cause failure due to fire. EDF uses the 'fire safety volume' concept, which takes into account these different points. The concept is illustrated in Figure 11.6 below.

Demonstration of the adequacy of fire protection measures is based on the study of reference fire scenarios used to determine how a fire would develop in a building and to assess its consequences for safety on a reasonably conservative basis. In this context, it is assumed that all the equipment fails in the fire compartment where the postulated fire has broken out.

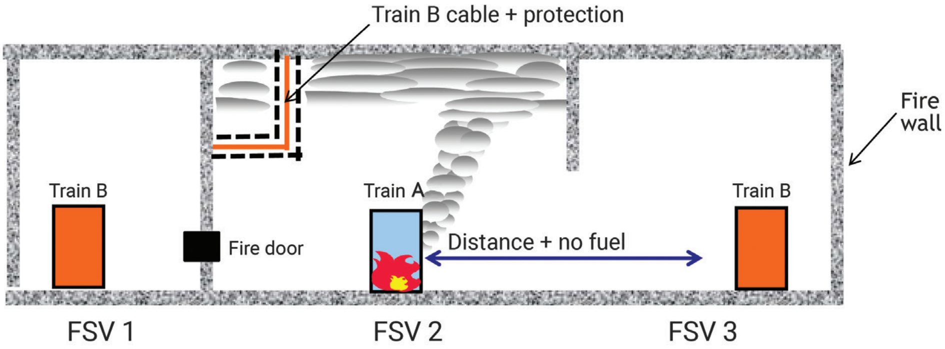


Figure 11.6. The 'fire safety volume' concept developed by EDF. Marc Henrio/IRSN.

The study of these fire scenarios must address all the effects induced by the fire (hot gases, mechanical effects due to the pressure variations produced, electrical equipment malfunctions due to soot, inflammation of unburned gases, etc.) and the ways in which the fire spreads. Modelling of these scenarios therefore assumes that the simulation tools used are capable of handling the complexity of the phenomena under study and the physical magnitudes to be characterized, while achieving the required accuracy. These simulation tools must be adequately validated based on the results of research and development programmes designed to ascertain thermal effects, the propagation of soot and hot gases, and the pressure levels resulting from the expansion of hot gases[409].

In addition to these scenarios, other complementary studies are conducted to examine scenarios taking into account the failure of certain protective measures (such as a fire door or an extinguishing system – aggravating failures) as well as fire scenarios affecting a set of rooms at the facility. This type of study is particularly pertinent because experience in operating nuclear power reactors has revealed the existence of compartmentation anomalies or nonconformities (for example, poorly sealed openings).

Fire scenarios are used to demonstrate that structures remain sufficiently stable under fire conditions. Generally, the fire resistance of specific protection measures such as walls, doors, ventilation or smoke extraction ducts, or any other means of fire protection, must be demonstrated by showing adequate qualification for the conditions in which they could be required to operate.

Despite the care taken to separate redundant trains and create fire compartments accordingly, it is difficult to completely exclude the possibility of simultaneous damage to safety equipment in redundant trains, amounting to fire[410] common modes. Fire

[409] For more information, see Current State of Research on Pressurized Water Reactor Safety, Chapter 7, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

[410] Despite the precautions taken to separate redundant trains and create fire compartments, there are 'convergence points', such as the control room or the presence of several sensors on the same section of duct, which offer potential for common-mode failures due to fire.

scenarios are used to identify these fire common modes and, after functional analysis, to identify any common modes that need to be addressed so that appropriate corrective measures can be taken.

To guarantee the effectiveness of the fire protection systems over time, the operator sets up a programme of inspections, periodic tests and maintenance for these systems. This programme is supported by providing training and refresher courses for personnel and organizing periodic exercises.

While based on deterministic principles, fire risk control at nuclear power plants is also demonstrated by special 'probabilistic safety analyses' (Fire PSAs – see Chapter 14) which identify system failure sequences leading to core melt. A probabilistic safety analysis of fire risk covers possible failures of fire protection measures (such as detection or extinguishing systems), as well as human error due in particular to the stress caused by a fire.

In the French nuclear power plant fleet, fire risk control was addressed in a fire-fighting action plan from 1998 to 2006. Since then, as successive ten-yearly reactor reviews have taken place, EDF has defined and introduced various sets of changes.

Operators give constant attention to the question of fire risk. Outbreaks of fire regularly occur in French nuclear reactors, with consequences that have varying degrees of severity. Some examples are:

- an incident that occurred in July 1999 at the Bugey nuclear power plant, where a common cause (an electrical fault in a switchboard at the pumping station) led to two electrical faults and two almost simultaneous outbreaks of fire in Unit 3, in different and geographically separate 'fire safety volumes';
- an electrical cable fire in 2004 caused by overheating in an opening between the turbine hall and the electrical building of Unit 2 at the Cattenom nuclear power plant;
- an oil fire in 2012 in the reactor coolant pump of the Unit 2 building at the Penly nuclear power plant.

11.7. Explosion protection

In a nuclear power plant, a distinction is made between conventional explosion risks[411] and explosion risks related to a core-melt situation that can lead to the formation and release of hydrogen – or even a 'steam explosion' (stemming from a thermodynamic interaction between molten materials and coolant). Steam explosions are discussed in Chapter 17.

[411] Sudden release of energy leading to propagation of a flame front and an overpressure wave. This is described as a deflagration if the speed of the flame front is subsonic, i.e. below the speed of sound in the ambient environment, and a detonation if the speed of the flame front is supersonic; the flames then accompany the overpressure and a shockwave forms, which can cause significant damage.

In the mid-1990s, the application of 'explosive atmospheres' regulation prompted EDF to improve measures to control explosion risks for worker protection. At the time there was no formal procedure for assessing the safety risks related to an explosion.

An event that occurred on 21 October 1998 in Unit 4 of the Chinon B nuclear power plant played a particularly important role in improving the way explosion risks at nuclear power plants were taken into account. Work was scheduled in the nuclear auxiliary building on a valve in a hydrogen line supplying the chemical and volume control system tank. The workers intervened on the wrong component and dismantled the valve's twin, belonging to Unit 3, which was in operation. This line contained pressurized hydrogen. The error caused a major hydrogen leak, detected both by the workers and by the hydrogen detectors in the adjacent room, which sent an alarm to the control room. Having requested evacuation of the buildings, a floor operator confirmed the hydrogen leak after observing a drop in pressure on the corresponding line, and shut down the hydrogen supply to Unit 3. Luckily the leak, which lasted for approximately 30 min, did not cause an explosion, even though the hydrogen detection alarm remained active for around 35 min.

This event highlighted the importance and necessity of more exhaustive assessment of explosion risks at nuclear power plants. The analysis of the event's potential consequences showed that a hydrogen cloud explosion could have led to the loss of numerous systems and components important to safety.

This event, which happened between two oil-breaker explosions on the Tihange site (Belgium) in 1996 and the Gravelines site in 2001, prompted EDF in 2004 to introduce a formal explosion risk assessment procedure in a 'baseline study' that aimed to take into account safety risks more effectively. The procedure aims to demonstrate that, if there is a hydrogen leak and explosion, the reactor can be maintained in or restored to a safe state.

Generally, explosion risk assessments are conducted in several stages.

The first stage consists in identifying all possible sources of explosions. In nuclear power plants, the main risks are associated with the use of hydrogen in certain processes. Hydrogen is used in the reactor building to control water chemistry in the reactor coolant system. It is also used to cool the electric generator in the turbine hall. For these purposes, hydrogen circulates through a piping system that takes its source from the gas storage areas outside the buildings. The explosion risk assessment must consider the possibility of hydrogen release at any point along these pipelines.

Some rooms also accommodate processes that generate hydrogen, for example:

- rooms containing electric batteries, which release hydrogen as they are being charged;
- the electrochlorination process used specifically on sites beside the sea.

Explosion risks can also be associated with:

- transformers and circuit breakers using oil as a dielectric;

- chemical incompatibilities between certain reagents used in processes;
- the temporary presence of explosive gas tanks in certain rooms within the nuclear island (such as acetylene cylinders used during maintenance work);
- the use of flammable liquids (solvents, fuel for diesel generators).

Once this equipment has been identified, measures to prevent situations likely to present an explosion risk must be examined. Application of the procedure to pipelines containing hydrogen leads to taking measures to protect hydrogen lines from hazards such as earthquakes or high-energy line breaks (HELB), corrosion, incorrect dismantling of certain equipment, impacts or fire. Hydrogen lines are thus generally designed to withstand earthquakes. The installation of pipe-whip restraints around high-pressure pipes can prevent the corresponding hazard risk (HELB). The risk of corrosion can be addressed at the design stage through the choice of materials or during operation by applying inspection and maintenance procedures.

In addition to these preventive measures, other measures are taken to limit the flammable volume likely to be generated if there is an accidental hydrogen release. These might include, for example, the installation of:

- ventilation systems in areas where an explosive atmosphere could develop (rooms containing batteries, rooms that hydrogen lines pass through),
- systems to limit the leakage rate from hydrogen lines,
- gas detection systems and safety systems in case an abnormally high hydrogen concentration is detected, etc.

In addition to these measures, it is also possible to reduce sources of ignition. There are components and systems, such as lighting systems and pumps, designed to operate in specific environments and reduce sources of inflammation.

Finally, the explosion risk assessment also covers the risk of degraded situations arising due to failure of the above measures, and examines the possible consequences of an explosion for facility safety, in particular any resulting common modes. The calculation methods used in this case must be sufficiently bounding to cover the many uncertainties inherent in the study of the complex phenomena involved. The study of the consequences of an explosion is completed by a study of domino effects that could be envisaged. This is to verify that an explosion is not likely to damage equipment which, if it failed, could cause one or more additional hazardous phenomena such as a second explosion or a fire.

If the consequences of the envisaged explosions appear to be unacceptable, further measures must be taken (to reduce their probability or mitigate the consequences).

As in the case of fire risks, because the safety demonstration for explosion risks relies on a set of physical and organizational measures, the operator must guarantee their effectiveness over time by implementing a programme of inspections, periodic tests and maintenance, as well as personnel training and regular exercises.

11.8. Internal flooding

As with the previous hazards, the risks associated with a major water spill inside the facility were not studied for the early units in the nuclear power plant fleet.

This question was handled according to the state of the art, with equipment, pumps and electrical cabinets often installed on small raised blocks. Rooms containing fluid-conveying pipes sometimes had drains, sumps and sump pumps; some floor openings were surrounded by low walls and were sealed with plaster.

A few key events drew attention to the risks associated with internal flooding. One occurred in October 1980 at Unit 2 of the Indian Point nuclear power plant in the USA (see the Focus feature below), and another took place in October 1989, at the Vandellos I nuclear power plant in Spain (GCR reactor[412]), where internal flooding by seawater was caused by a series of events: rupture of turbine blades, hydrogen leak and explosion, turbine lubricating oil fire, loss of power supply and instrument compressed air to several items of equipment involved in residual heat removal. The flooding endangered the operation of the plant emergency core-cooling-system pumps in the reactor building basement.

#FOCUS

Flooding in 1980 at the Indian Point nuclear power plant in the USA

The event affected Unit 2 of the Indian Point nuclear power plant in the USA (in the state of New York), a pressurized water reactor designed by Westinghouse rated at just over 1000 MWe[413]. A major leak of raw water used for cooling certain systems and equipment, without an intermediate pipeline, in a once-through system from the Hudson River, occurred in the containment. In this nuclear power plant (Figure 11.7), the reactor pit was the lowest point in the containment and the vessel lower head was itself below the lowest level of the rest of the facility. Several faults in the reactor pit and containment sump pumps and a lack of confidence among the operators regarding the water level indications in these sumps allowed the leak to develop. Four hundred cubic metres of water accumulated in the reactor containment.

The operators only reacted when one of the neutron flux chambers gave a manifestly abnormal signal because part of the corresponding equipment was flooded.

[412] Reactor operated using gas-cooled, graphite-moderated, natural uranium fuel (GCR: gas-cooled reactor).

[413] Permanent shutdown of the Indian Point plant was ordered in 2016.

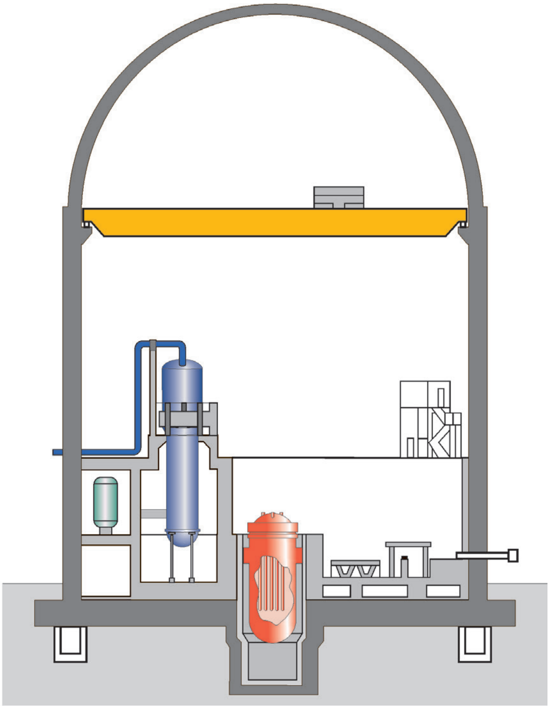


Figure 11.7. Reactor vessel layout at the Indian Point nuclear power plant. IRSN.

The reactor operated at power even though the vessel lower head, which was insulated, was under water. This was clearly not a normal situation.

The design and layout of equipment in the reactors of French nuclear power plants are significantly different from those at the Indian Point plant. Although an identical accident could therefore not be envisaged, it was still necessary to examine potential flooding more carefully.

Internal flooding that can occur in a facility in normal operation may be caused by:

- a pipe rupture or leak,
- a tank emptying,
- spraying by fixed fire protection systems,
- spraying by the containment spray system, including if the system starts up inadvertently.

In accident situations (category 3 and 4 operating conditions), internal flooding risks can be due:

- directly to the event in question; this is typically the case for loss-of-coolant accidents (LOCA),
- to a passive, long-term failure, in application of the single-failure criterion (see Section 7.2).

Generally, as with other hazards, the facility must be designed to guarantee in these situations:

- availability of the safety functions,
- prevention and mitigation of any release of radioactive substances.

The safety demonstration must substantiate that internal flooding will not lead to failures likely to compromise one of the safety objectives mentioned above. In particular, the retention of contaminated fluids inside buildings or structures must prevent groundwater contamination in the event of internal flooding.

When the redundant trains of a safety system are installed in physically separate rooms (in terms of flooding risk), the consequences of internal flooding likely to affect a single train are not studied. When redundant trains pass through the same rooms or connected rooms, measures must be taken (protection, monitoring systems, associated procedures) to guarantee reactor safety in the event of internal flooding. In this case it is necessary to consider:

- the envisaged flooding rate,
- the duration of flooding, which includes the time necessary to detect flooding and isolate the leak;
- the spread of flooding to other rooms; in this context, the leaktightness of seals (at openings) between rooms and between civil works (expansion joints) must be examined.

It is necessary to determine how flooding spreads, taking into account the different possible routes of the water through:

- tunnels and gutters,
- staircases and holes in floors (openings, floor drains, sleeves, etc.) and openings in walls,
- drainage systems,
- connections between rooms and with other buildings (ventilation ducts, links between tunnels and buildings, spaces under doors).

The equipment used to demonstrate that internal flooding risks are under control must meet the following specific requirements:

- ability to operate in special conditions (humidity, etc.),
- ability to operate after spraying or immersion.

In addition, the ability of civil works and doors to withstand the water load must also be examined.

Protection against internal flooding may be provided by taking the following measures:

- installing safety trains in rooms that cannot be simultaneously affected by a flood,
- installing drainage systems in rooms subject to flooding,
- installing structures (door thresholds, low walls, sloping floors, etc.) to limit the spread of flooding to a single safety train or avoid groundwater contamination,
- raising equipment in rooms off the floor or installing protective structures if it has not been demonstrated that the equipment is capable of functioning when submerged,
- installing leaktight retention systems around tanks,
- installing sump pumps and water level sensors at the bottom of buildings to detect flooding.

In French nuclear power plants, however, operating experience has shown that it is sometimes difficult to predict where water will run, especially when there are compliance gaps involving protection systems. For example, on 30 September 2005, in Unit 1 at the Nogent-sur-Seine nuclear power plant, the blowdown valves on the main feedwater system (MFWS) pipes located on the roof of the electrical building had been left open which, due to cumulative compliance gaps concerning civil works, caused water to flow into the safety instrumentation and control system rooms several levels below, leading to a reactor trip and spurious safety injection. Similarly, on 9 April 2014, a tank in the turbine hall of Unit 1 at the Fessenheim nuclear power plant overflowed due to obstruction of the tank's overflow pipe, causing water to flow into the electrical building and, because the cable penetrations were not leaktight, it flowed into the safety instrumentation and control system rooms several levels below. The failures observed caused the operating crew to shut down the reactor.

The procedure has gradually been enhanced and reorganized; for the safety reassessment studies carried out during the fourth ten-yearly outage of the 900 MWe reactors, it includes:

- identification of all possible sources of internal flooding, such as high- and medium-energy pipes, tanks, or spurious spraying by the firefighting système;
- for each source studied, identification of flooding scenarios, with calculation of the volume of flood-water accumulated until the source has been isolated and the height reached by flood-water in the various flooded rooms in each of these scenarios; the routes of propagation considered (vertical or horizontal) consist of doors, ducts, penetrations between rooms or buildings, floor drains, etc.;

- the identification of sprayed, submerged or struck equipment in the event of pipe whip (from high-energy pipes);
- taking into account the most penalizing aggravating failure.

Chapter 12
Providing for External Hazards

12.1. General considerations on providing for external hazards

General considerations on providing for internal and external hazards were presented in the previous chapter. This chapter illustrates how these general principles apply to just a few external hazards, knowing that other external hazards (such as tornadoes) are also the subject of studies, research and regulations. Deterministic and probabilistic approaches are applied to the hazards presented in this chapter and to the other external hazards not discussed in this book.

Since the first high-power nuclear power plants were designed – in the early 1970s in France – special consideration has been given to seismic risks, which have been explicitly taken into account in the design of equipment important to safety, civil works (such as reactor buildings), and also the equipment installed inside these structures. Similarly, the site platform elevation of nuclear plants located on coastal or river sites is dictated by the risks of external flooding.

However, these are not the only risks related to the environment.

As mentioned in Section 11.1, external hazards can be of natural origin, as in the case of earthquakes, strong winds, storms, tornadoes, lightning, floods, extremely cold weather or heatwaves, volcanic activity, meteorites, etc., or of human origin, as in the case of aeroplane crashes, explosions, off-site fires or release of toxic gases. But they do not all have the same adverse effects on facilities, which has led to specific approaches for dealing with each type of hazard. Certain natural hazards can simultaneously affect redundant or diversified trains of safety systems, multiple safety systems, multiple units on the same site, and infrastructure on and around the site (such as the power supply grid), which is especially the case for earthquakes.

The severity of some external hazards can change during facility lifetime (climate conditions, industrial risks, etc.). It is necessary to plan ahead for these as far as possible, knowing that periodic reassessments are designed to regularly examine these changes and take appropriate measures, as necessary.

The general purpose of systems provided to protect nuclear reactors from internal and external hazards is to keep them from compromising the availability of equipment necessary to perform safety functions, especially the fundamental safety functions, taking into account the associated study rules[414] and the direct or indirect effects of these hazards.

The reference characteristics for external hazards are defined using probabilistic methods (in the case of aeroplane crashes and explosions), or deterministic methods, or a combination of both (in the case of floods, where studies are based on scenarios and statistical methods).

For design-basis reference hazards, a maximum frequency of 10^{-4} per year (per hazard) is recommended as the target reference value in the Issue T section of the WENRA reference levels, updated in 2014. However, it is not always possible, based on historical data, to determine for a given external hazard the event having a return period compatible with a value of 10^{-4} per year; the same WENRA document states that "where it is not possible to calculate these probabilities with an acceptable degree of certainty, an event shall be chosen and justified to reach an equivalent level of safety." ASN Guide No. 22, issued in 2017, takes the same approach[415]. The examples and explanations below show the approaches taken until now, adding fixed margins to the intensity values derived from known, available historical data (generally for 1000-year return periods).

Lastly, the objectives set in ASN Guide No. 22 for new reactor designs can also serve as a reference during periodic reviews of reactors already in operation. For design extension conditions (DEC, see Section 6.5), the analysis of low-probability hazards and facility improvements that could reasonably be made to ensure protection against these hazards should show, as much as possible, that there are sufficient margins to avoid cliff-edge effects that could lead to loss of the fundamental safety functions[416]. Following on from the complementary safety assessments carried out in the wake of the Fukushima Daiichi nuclear power plant accident (which cover extreme hazards), ASN Guide No. 22 recommends that design extension conditions for pressurized water reactors take into account natural hazards of greater severity than the hazards

[414] See Section 11.1 for a special focus on provisions for the most penalizing aggravating failure.

[415] Sections 3.3.3.2.7 and 3.3.3.2.8 of the guide.

[416] ASN Guide No 22, Section 3.4.1.2.

chosen for the design reference domain. ASN Guide No. 22 contains the following recommendations:

- "Taking into account external natural hazards in the design extension conditions contributes to the objective of minimizing risks [...] both to prevent core melt and to limit the measures required to protect the population in situations with core melt."
- "When identifying the external natural hazards to be considered in design extension conditions, the severity of the hazard based on its estimated annual exceedance frequency must be established when possible."
- "For external natural hazards where the annual exceedance frequency of the hazard cannot be calculated, or when uncertainty for this value is too high, an 'event' of greater severity than the one considered in the design reference domain must be chosen and substantiated."

The specific approaches used for a few external hazards are explained in detail in the rest of this chapter, with special attention given to the manner in which the physical characteristics of hazards are chosen in the course of equipment design.

12.2. 'Climate watch' implemented by EDF

Because of climate change and to prepare for future eventualities, EDF has set up a 'climate watch' for external hazards such as external floods, rain and (extreme) ambient air temperatures. In the case of ambient air temperatures, this climate watch relies particularly on measurements taken by the nationwide weather network of Météo France.

The climate watch allows EDF to determine which new data are to be taken into account during the ten-yearly reactor periodic outages, including any (forecast) trends for at least the next ten years and the associated levels of uncertainty. This approach, implemented during the fourth ten-yearly outage of 900 MWe units, is depicted in Figure 12.1.

12.3. Earthquakes

▶ Taking into account earthquakes when designing nuclear power plant reactors

Until the 1970s, early nuclear facilities in France were designed according to existing seismic design rules[417], which were not specifically oriented toward nuclear facilities.

[417] AS 55 recommendations (from 1955), established following the 1954 earthquake at Orléansville in Algeria, seismic design rules PS62, 64, 67, 69, etc.

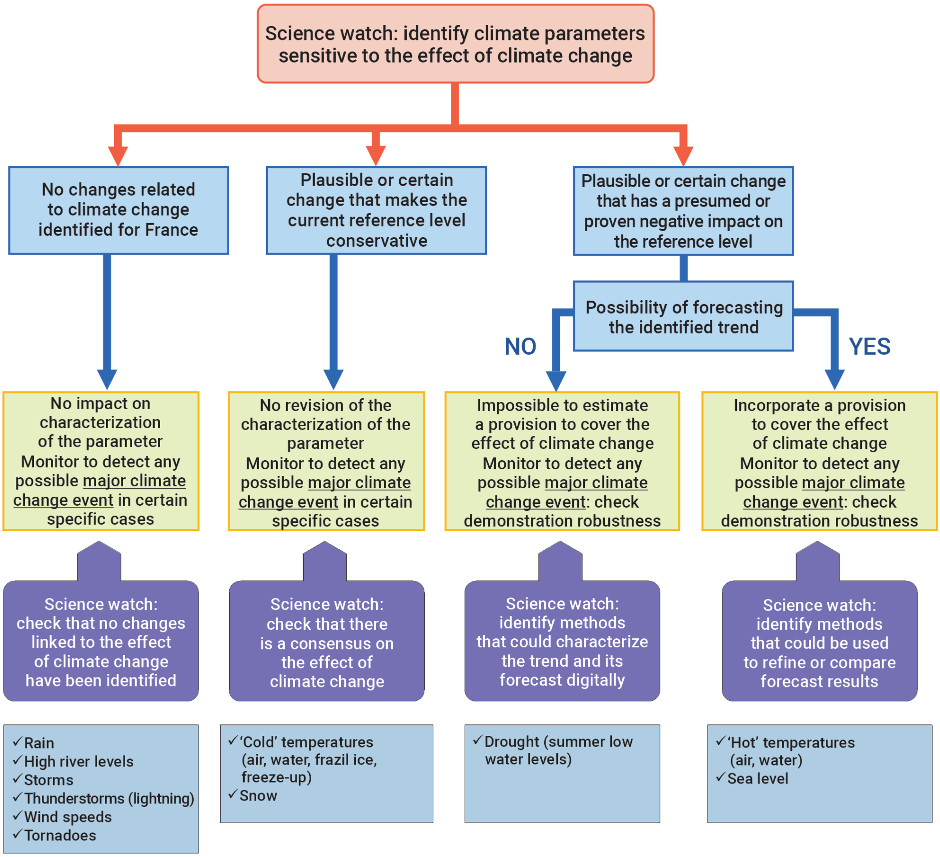

Science watch: identify climate parameters sensitive to the effect of climate change
No changes related to climate change identified for France
Plausible or certain change that makes the current reference level conservative
Plausible or certain change that has a presumed or proven negative impact on the reference level
Possibility of forecasting the identified trend
NO
YES
No impact on characterization of the parameter Monitor to detect any possible major climate change event in certain specific cases
No revision of the characterization of the parameter Monitor to detect any possible major climate change event in certain specific cases
Impossible to estimate a provision to cover the effect of climate change Monitor to detect any possible major climate change event: check demonstration robustness
Incorporate a provision to cover the effect of climate change Monitor to detect any possible major climate change event: check demonstration robustness
Science watch: check that no changes linked to the effect of climate change have been identified
Science watch: check that there is a consensus on the effect of climate change
Science watch: identify methods that could characterize the trend and its forecast digitally
Science watch: identify methods that could be used to refine or compare forecast results
✓Rain
✓High river levels
✓Storms
✓Thunderstorms (lightning)
✓Wind speeds
✓Tornadoes
✓'Cold' temperatures (air, water, frazil ice, freeze-up)
✓Snow
✓Drought (summer low water levels)
✓'Hot' temperatures (air, water)
✓Sea level

Figure 12.1. Logic diagram summarizing the approach used to take into account climate change during the fourth ten-yearly outage of 900 MWe reactors. IRSN.

In 1974, when the design and safety studies were carried out for the first pressurized water reactors built under licence from Westinghouse, the CEA's Nuclear Safety Department[418] wrote a report, DSN 50, entitled Seismic Protection for Power Plants (*Protection des centrales vis-à-vis des séismes*). This report provided a survey of French practices (on research reactors or the PHENIX fast-neutron reactor) as well as foreign practices in the field (particularly in the USA) and put forward a number of proposals, with a particular focus on determining the ground response spectra[419] to be used for assessing the 'response' (or behaviour) of structures under earthquake conditions.

These elements would constitute the working basis for facility operators and were the precursors of fundamental safety rule RFS I.2.c, issued in 1981 by the Central

[418] IPSN was only created within the CEA in 1976.

[419] Response, in terms of acceleration, of oscillators having different natural frequencies, subject to the earthquake under consideration.

Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN), applicable to pressurized water reactors. This fundamental safety rule recommends an 'acceptable' deterministic method for determining the seismic movements to be taken into account when designing reactors that are capable of withstanding seismic sollicitations[420].

The recommended method is deterministic in the sense that it assumes that earthquakes similar to the historically known seismic events (in terms of 'intensity' according to the MSK[421] scale – see below) could occur in the future, with their epicentre in more penalizing locations as regards their effects on the site, while remaining compatible with geological and seismic data.

Seismic 'accidents' and tectonic zones must be studied, as well as historical earthquake data (accessible in archives for the last five to ten centuries) and instrument data[422] (see Figure 12.2). The investigation must focus primarily on the site, but should extend as far as necessary, since borders are obviously irrelevant here.

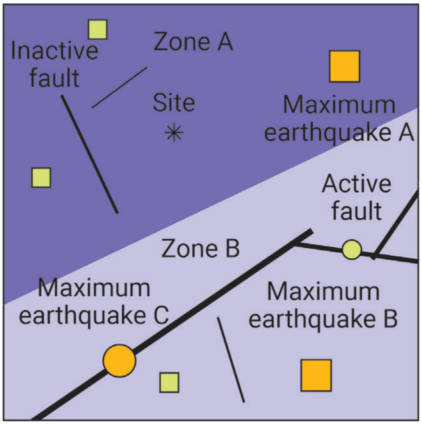


Figure 12.2. Example of geological and seismological data to be taken into account when siting a nuclear facility. Georges Goué/IRSN.

For the site in question, this approach defines one or more maximum historically probable earthquakes (MHPE[423]) likely to produce the greatest effects on the site.

In the 1960s, Professor Jean-Pierre Rothé at the University of Strasbourg produced a map of historical earthquakes (since the year 1021) that have occurred in France and neighbouring countries, with their intensity where it could be determined. He produced

[420] In 1992, fundamental safety rule RFS I.1.c extended the application of this method to all basic nuclear installations, including research reactors.

[421] Earthquake intensity scale developed by Medvedev, Sponheuer and Karnik.

[422] Derived from measurements. The first seismology station in France was set up in Strasbourg in 1892. As at 2020, France had approximately 200 recording sites.

[423] Sometimes referred to as a 'basic earthquake', as opposed to a seismic margin earthquake.

a map of the maximum intensities observed, which was used as a reference document for the seismic protection of nuclear facilities. A more comprehensive and precise study of France was subsequently conducted some time around 1980, as part of a seismic zoning process, producing a seismic map of metropolitan France. This work was carried out by the French geological survey office (*Bureau de recherches géologiques et minières*) BRGM in collaboration with EDF and CEA. Other work has subsequently been carried out on the subject. The outcome of work begun more than 30 years ago, the French national macroseismic database of historical and contemporary earthquakes, known as SisFrance (BRGM/EDF/IRSN), is continuously updated to guarantee the best state of knowledge of macroseismicity in France. Supported by the French Ministry of the Environment, SisFrance was made accessible on line in 2002. The database contains information (dates, epicentre positions, local intensity values, etc.) on earthquakes in France.

It has thus been possible to collect consistent descriptions of historical seismic accidents and tectonic zones throughout France. 'Seismotectonic zones' have been defined, which are volumes of the Earth's crust with homogeneous seismogenic potential.

The MHPEs for any site under study are derived by moving, or 'translating', their epicentres as follows (see Figure 12.3):

- it is considered that the historical earthquakes in the seismotectonic zone of the site could occur underneath the site (maximum earthquake marked 'A' in the diagram);
- it is considered that the historical earthquakes in a neighbouring seismotectonic zone could occur at the nearest point in that zone to the site (maximum earthquake marked 'B' on the diagram, with earthquake 'C' moved along its fault).

For all cases under study, it is considered that the historical earthquakes attributable to a specific seismic accident could occur at the closest point of that accident to the site.

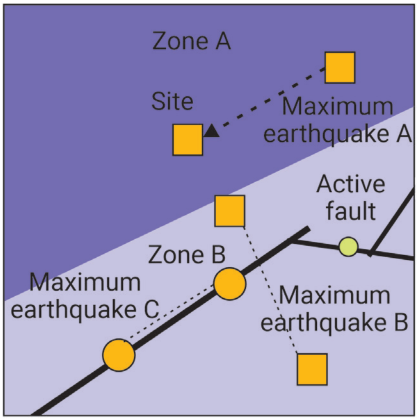


Figure 12.3. Determining MHPEs. Georges Goué/IRSN.

For each of the MHPEs, the fundamental safety rule defines a seismic margin earthquake (SME), derived from the MHPE by a simple relationship in terms of intensity on the MSK scale (see the Focus feature below).

$$I_{SME} = I_{MHPE} + 1$$

#FOCUS

Earthquake intensity and magnitude

The intensity of an earthquake at a given point on the ground corresponds to the evaluation of the effects of this earthquake. The reference scale used to design basic nuclear installations in France is a 12-degree scale known as the Medvedev-Sponheuer-Karnik (MSK) scale, developed in 1964 and derived from the Mercalli scale. Intensity values are expressed in Roman numerals. In the MSK scale, a one-degree increase generally corresponds to multiplying ground acceleration by a factor of two.

Degrees on the MSK scale correspond to the perceived effects expressed as follows:

MSK scale	Perceived effect
I	Not felt, registered only by seismographs
II	Felt only by individuals at rest. No effect on objects
III	Felt indoors by a few. Hanging objects swing slightly
IV	Felt indoors by many and felt outdoors only by very few. A few people are awakened. Moderate vibration. Hanging objects swing. Light furniture shakes visibly in a few cases
V	Felt indoors by most, outdoors by few. Many sleeping people awake. Strong shaking or rocking of the whole building, room or furniture. Hanging objects swing considerably. In a few cases window panes break. Slight damage to a few poorly constructed buildings
VI	Felt by most indoors and by many outdoors. A few persons lose their balance. Small objects may fall and furniture may be shifted. Farm animals may be frightened. Visible damage to masonry structures, cracks in plaster. Isolated cracks on the ground
VII	Most people are frightened and try to run outdoors. Furniture is shifted and may be overturned. Objects fall from shelves. Water splashes from containers. Serious damage to older buildings, masonry chimneys collapse. Small landslides
VIII	Many people find it difficult to stand, even outdoors. Furniture may be overturned. Waves may be seen on very soft ground. Older structures partially collapse or sustain considerable damage. Large cracks and fissures opening up, rockfalls
IX	General panic. People may be forcibly thrown to the ground. Waves are seen on soft ground. Substandard structures collapse. Substantial damage to well-constructed structures. Underground pipelines ruptured. Ground fracturing, widespread landslides

MSK scale	Perceived effect
X	Masonry buildings destroyed, infrastructure crippled. Massive landslides. Water bodies may be overtopped, causing flooding of the surrounding areas and formation of new water bodies
XI	Most buildings and structures collapse. Widespread ground disturbances, tsunamis
XII	All surface and underground structures completely destroyed. Landscape generally changed, rivers change paths, tsunamis

This scale, which represents surface effects at a particular location and their impact on people, buildings and the environment, should not be confused with the scale of magnitude, which represents the energy released by an earthquake. The magnitude of an earthquake is calculated mainly from measurements taken by seismometers using a logarithmic equation based on the measured amplitude of the ground movement. Magnitude was introduced in 1935 by Charles Francis Richter for earthquakes in California (also known since then as 'local magnitude' ML). However, its use is limited and there are now several magnitude scales adapted to the different types of earthquakes and waves recorded.

In practice, the magnitudes (ML) observed since seismographs were installed at the start of the last century have ranged from -1 for the small tremors recorded by very sensitive seismographs near an epicentre, to more than 9 for the strongest earthquakes in Chile, Alaska, Russia, Japan and Indonesia.

There is no simple correspondence between the intensity scale and the magnitude scale because, for the same magnitude at the epicentre, the effects at the surface and in a particular place (intensity) depend in particular on the epicentre depth, the distance of that place from the epicentre, and the soil type.

The SME rather than the MHPE is used for designing nuclear power plants because, as knowledge has developed, there have been cases identified in France where the MHPE has been underestimated.

Moving the epicentre so that it is on the exact location of the facility or closer to it contributes to ensuring that the seismic movements used for design purposes are bounding.

Thus, for France as a whole, the estimated frequency for an SME earthquake for a particular site is around 10^{-4} per year[424].

[424] According to the most recent estimates, the frequencies associated with SME-level seismic movements appear to be between a few 10^{-3} per year and a few 10^{-4} per year, depending on the general seismic activity of the zone.

Based on the seismotectonic data for France – a country of low to moderate seismicity[425] – the reactors in the nuclear power plant fleet have therefore been designed for seismic margin earthquakes of intensities ranging from VI (Dampierre-en-Burly site) to VIII-IX (Cruas-Meysse site).

The intensity of an earthquake is not information that can be used directly in facility design. For each site, the magnitude of the SME is derived using a correlation based on intensity and distance from the source (hypocenter). An oscillator[426] response spectrum is then produced, giving the acceleration, velocity and vertical and horizontal displacement at ground level for each frequency. The response spectrum is calculated as a function of the magnitude and the distance from the source of the earthquake, using a seismic movement prediction equation based on earthquake recordings from around the world. RFS I.2.c, published in 1981, used this practice to define a 'distant earthquake' spectrum, and also proposed a standard 'close earthquake' spectrum, since these two types of earthquakes[427] can affect structures differently.

Because the spectra associated with real earthquakes are very complex, the decision was made for French nuclear power reactors to use one or more standard spectra derived from the U.S. NRC Regulatory Guide 1.60, which bounds the spectra characteristic of the seismic margin earthquakes on the site by appropriately setting acceleration at infinite frequency (also known as the peak ground acceleration, or PGA). As part of the standardization of French reactors, the spectra used were standardized (design response spectra) for each reactor series. For each site studied, the standardized spectra of the corresponding series were checked to make sure they covered the spectra of SMEs at the site location. The standard setting was 0.15 g.

For some reactors in the Paris Basin, a region of particularly low seismicity, a less stringent 'sub-standard' was used. Special arrangements were also made for sites with characteristics that were not covered by the bounding conditions defined for the standard plant unit series. These are cases where the ground may consist of particularly hard rock; or where shallow earthquakes may exist, inducing significant acceleration, velocity and displacement in high frequencies that are not within the bounding limits of the standard spectrum; or where seismic margin earthquakes have an intensity greater than VIII on the MSK scale.

[425] With some destructive earthquakes, such as in Basel in 1356 (near the French border), Bigorre in 1660, Remiremont in 1682, Bouin in 1799, in the Mediterranean sea off Italy's Ligurian coast in 1887, Lambesc in 1909, and Arette in 1967. In France, seismicity is low in the Paris Basin and in the Aquitaine Basin.

[426] Mass-spring system.

[427] 'Close earthquakes' are earthquakes of low magnitude occurring less than 15 km from the facility in question, affecting structures to a greater extent at high frequencies. 'Distant earthquakes' are of high magnitude and occur more than 15 km away, with a greater impact on structures at low frequencies.

▶ Evolution of the approach

Since the 1980s, practice has gradually moved to the classification of earthquakes according to a scale known as the surface-wave magnitude scale (Ms)[428] and a scale known as the moment magnitude scale (Mw)[429]. Since C. F. Richter (see the Focus feature above), new definitions of magnitude have been proposed, mainly to characterize events regardless of the region of the world where they occurred and the type of instruments that recorded them (instruments have evolved considerably since 1935), and to estimate physically, rather than empirically, the size of the rupture.

In 2001, a new fundamental safety rule, RFS 2001-01, was issued by the French Nuclear Installations Safety Directorate following several years of discussions with the designers and operators of nuclear facilities, in particular. This new fundamental safety rule maintained a deterministic approach, but also introduced further developments about how paleoearthquakes and site effects should be taken into account (see the Focus feature below).

Expressed in terms of surface-wave magnitude, the increase in a unit of intensity between the MHPE and the SME is:

$$Ms_{SME} = Ms_{MHPE} + 0.5$$

RFS 2001-01 also recommends an updated equation for predicting seismic movement that takes into account more earthquakes than the equation recommended by the 1981 fundamental safety rule and covers both ‘distant earthquakes’ and ‘close earthquakes’.

For paleoearthquakes, the new fundamental safety rule recommends examining whether there are active faults near the chosen site with evidence of surface ruptures and a risk (in terms of the return period and magnitude associated with the fault dimensions) that they could cause further earthquakes that would affect the site.

Finally, for sites with a very low seismic risk, a fixed minimum spectrum is recommended by RFS 2001-01, for which the peak ground acceleration (PGA) is set to 0.1 g.

For the French nuclear power plant fleet, RFS 2001-01 is used as a reference during the seismic reassessments associated with the ten-yearly reactor outages, which also take into account, as necessary, the changes mentioned earlier in the seismic zoning of metropolitan France. These seismic reassessments have played a particularly signif-

[428] The magnitude Ms, or surface-wave magnitude, is similar to the local magnitude except that it uses only one type of wave, the surface wave, from the seismogram. This magnitude can be used to characterize earthquakes that will generate a large number of surface waves (for example, earthquakes on strike-slip faults such as the San Andreas Fault in California and the North Anatolian Fault in Turkey). However, it cannot be used for deep earthquakes that generate very few surface waves, although they are the largest earthquakes.

[429] This is why, in 1977, Hiroo Kanamori introduced the Mw magnitude, or moment magnitude. Its estimation is based on the physics of the rupture and is directly proportional to the energy released during the earthquake rupture, and therefore to its size.

icant role in the structural reinforcement implemented at the Fessenheim and Bugey sites[430].

For the Flamanville 3 EPR design, significant margins were used, taking a fixed design-basis spectrum, known as EUR[431], set at 0.25 g (the SME for the Flamanville site is 0.16 g).

#FOCUS

Paleoearthquakes – Site effects

Paleoearthquakes are strong earthquakes that happened in the distant past (tens or hundreds of thousands of years ago) that are identifiable from the traces they have left behind in geological deposits. The purpose of studying them is to understand the occurrence of such earthquakes and to characterize them so as to gain more complete knowledge of a site's seismicity beyond the period for which instrument data (from the last century) or historical records (roughly the last millennium in France) exist.

The site effects to be studied are potential amplifications of seismic movement due to the existence of a layer of soil with low mechanical resistance that lies near the surface (see for example Figure 12.4). The equation in RFS 2001-01 for the prediction of seismic movement can be used to calculate the response spectra for two site conditions, depending on the mean velocity of the shear waves measured in the first 30 m of depth.

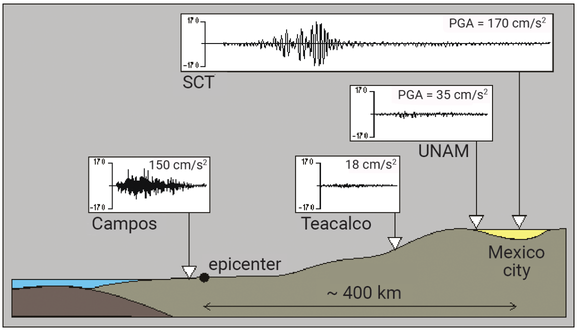


Figure 12.4. Example of site effects in the lake area of Mexico City (1985). Characterization of the non-linear behaviour of the ground under seismic load. J.F. Semblat, A. Pecker (IUSS Press, 2009).

[430] Including the post-Fukushima assessments (spectra for the hardened safety core, a topic discussed in greater detail in Section 36.6.5.).

[431] European Utility Requirements (requirements defined by a group of European power utilities).

In some specific cases, because of complex geometry or very thick sedimentary formations (as in a sedimentary basin), the duration of seismic movement may be amplified or extended. These effects, known as site-specific effects, are not caused solely by the properties of the ground in the first 30 m below the surface.

As stated above, because all the components of a facility are subject to the effects of seismic movement, facility safety relies on the appropriate design[432] of a first set of systems and components (based on the 'load case' approach) selected to ensure, in the case of a nuclear reactor, that the facility can be brought to a safe and stable state, considering different initial situations of the reactor, including accident situations. But another type of reasoning has also been applied[433], based on the 'earthquake as an event' approach (or the 'event-initiating earthquake' mentioned previously in Section 11.1). In this case, special attention is given to a second set of systems and components that must be designed in such a way that they cannot damage the first set under earthquake conditions (due to failure or falling, for example).

Whether equipment will behave correctly under seismic conditions can be verified by means of calculations (in the case of civil works and steel structures) or by full-scale tests conducted on a shake table for equipment such as electrical cabinets.

To determine the seismic loads that the equipment is subject to, two particular phenomena must be taken into account:

- soil-structure interaction (for civil works);
- the transmission of motion from building foundations to the different structural elements on which the equipment is installed, which generally leads to an amplification of acceleration from the foundation level to the higher parts of the building[434].

It is acceptable practice to study the 'response' of structures using (elastic) linear behavioural models. Incursions into the plastic domain can be treated on a case-by-case basis depending on the damage to structures considered permissible.

Among the components studied using the 'earthquake as an event' approach, special attention must be given to overhead cranes. A falling crane or crane trolley can cause significant damage. Preventing the crane or its trolley from falling, regardless of the cause, is therefore essential and must be kept in mind throughout design, sizing (particularly with regard to earthquakes), manufacturing (in compliance with proven best practice) and in-service inspections (including regulatory inspections of lifting

[432] This subject is approached in particular in ASN Guide 2/01 of 26 May 2006, on taking into account seismic risk in the (seismic) design of civil works at basic nuclear installations, except for facilities used for long-term disposal of radioactive waste.

[433] This approach was applied from the design phase for the N4 reactor series and then retrospectively, during periodic reviews of the first units built in the 1970s.

[434] The transmission of motion leads to the definition of what are known as 'floor spectra'.

equipment and auxiliary items). Operating rules can also be introduced to keep any movements over risk zones to a strict minimum, or measures can be taken to ensure cranes never pass over certain components during reactor states where those components must be available in order to comply with the safety demonstration.

Dynamic loads on structures in a nuclear power plant can be modified by placing special support items between the ground and these structures, consisting of reinforced concrete pads topped with elastomer bearings, which are horizontally very flexible and vertically very rigid. There are two types of bearing pads:

- purely elastic pads, such as those used for the Cruas-Meysse nuclear power plant;
- elastic pads with sliding plates that can accommodate larger movements, such as those used for the units at the Kœberg nuclear power plant (South Africa) designed by Framatome, built on a site with challenging seismic characteristics.

In both cases, the whole nuclear island is built on a single basemat to eliminate the problems posed by interconnections between separate buildings (this is also the case with the Flamanville 3 EPR).

The reactors in the French nuclear power plant fleet are also equipped with seismic instrumentation – following the recommendations of a 1984 fundamental safety rule on the subject (RFS I.3.b). If earth tremors occur at a site, this instrumentation provides the operator with data on the activity, in terms of the seismic movements that the items important to safety are subject to, for comparison with the seismic movements used as the design basis for the facilities. The operator can then decide whether to pursue reactor operation on the site in question and under what conditions, if any (preliminary checks on certain structures, etc.).

The seismic instrumentation installed includes a number of accelerometers appropriately positioned in the buildings and in 'free-field' locations. An alarm is triggered in the control room when a measured acceleration exceeds 0.01 g.

In the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, applicable to the EPR, an 'inspection earthquake' level of 0.05 g is given. The guidelines state that "after the occurrence of an earthquake up to this level, no verification or inspection of the components important to safety would be needed prior to returning the plant to or maintaining it in normal operation. However, adequate provisions must be implemented in the design phase to allow for any inspections and tests necessary if this acceleration threshold is exceeded."

▶ Lessons learned from the Fukushima Daiichi nuclear power plant accident and evolution of the approach to seismic risk

The accident in March 2011 at the Fukushima Daiichi nuclear power plant raised questions about the risks associated with more severe external hazards than those used in the design basis for nuclear power reactors, which could also simultaneously affect all the facilities on a single site, particularly any risks associated with earthquakes.

The measures implemented in France for nuclear power reactors as a result of the complementary safety assessments carried out for this purpose are discussed in greater detail in Chapter 36. They are based particularly on the concept of a 'hardened safety core' that can withstand an earthquake of greater intensity than the SME. As part of these changes, EDF equipped its nuclear power reactors with a device that triggers a reactor trip if a seismic threshold is exceeded.

In terms of methodology, the French Nuclear Safety Authority (ASN) requires[435] that the earthquake used to design the hardened safety core components must:

– either "bound the seismic margin earthquake (SME) for the site, with a 50% margin",

– or "bound the spectra defined using a probabilistic approach for a 20,000-year return period",

– "take into account site-specific effects, namely the soil type."

In response to the second point, EDF implemented a probabilistic method for assessing seismic hazards, known as the PSHA[436].

This method, described here briefly, consists of the following steps (see Figure 12.5):

– first, all the geological, geophysical and seismological data to be used for assessing the recurrence rates of earthquakes must be collected, aggregating the 'instrument' data (taken from measurements that are only available for recent earthquakes) and historical data (derived from document archives);

– the next step is to select or develop seismotectonic models based on interpretation of the data collected. These models define 'seismic sources' consisting of either faults or geographical zones with seismic and geological properties considered to be homogeneous (seismotectonic zones). For each seismic source, the frequency of earthquakes is estimated as a function of their magnitude, depth, etc. The range of magnitude to be taken into account for the hazard contingency calculation is also defined;

– equations to predict seismic movement[437] are then selected. These are used to calculate the seismic movements for the site in question (in practice, a distribution characterized by a mean and a standard deviation) as a function of

[435] Decisions dated 21 January 2015.

[436] Probabilistic Seismic Hazard Assessment. The method consists (in this case) in assessing, for a 20,000-year return period, a response spectrum from oscillators for seismic movement with a 0.25% probability of being reached or exceeded during a 50-year period. The return period of an event that constitutes a stationary process considered to follow a Poisson distribution is equal to Tr = –duration/ln(1 – exceedance probability), i.e. in the case of hardened safety cores, 19,975 years = –50/ln(1 – 0.0025).

[437] Ground Motion Prediction Equations (GMPE).

the source parameters, such as magnitude and distance from the source. The variability of seismic movements is taken into account in the calculations by including predictions up to a set number of standard deviations;

- finally, the probability of a ground motion value being exceeded at the site is assessed. It is necessary to take into account ground characteristics underneath facilities because local geological conditions can alter the movements that structures are subjected to.

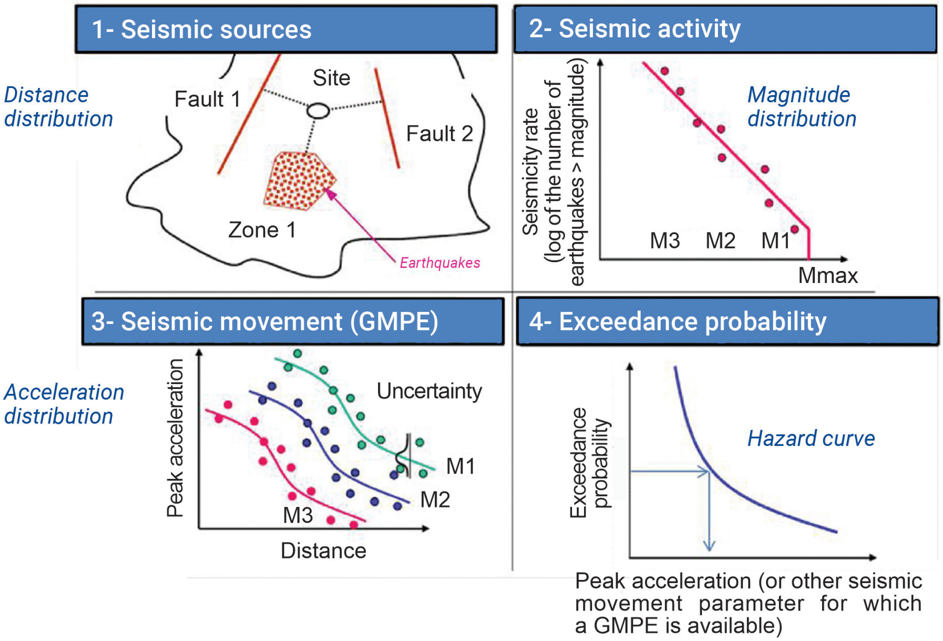

1- Seismic sources
2- Seismic activity
Distance distribution
Fault 1
Site
Fault 2
Zone 1
Earthquakes
Seismicity rate (log of the number of earthquakes > magnitude)
Magnitude distribution
M3
M2
M1
Mmax
3- Seismic movement (GMPE)
4- Exceedance probability
Acceleration distribution
Peak acceleration
Uncertainty
M1
M2
M3
Distance
Exceedance probability
Hazard curve
Peak acceleration (or other seismic movement parameter for which a GMPE is available)

Figure 12.5. Diagram showing the different steps of the PSHA method. Oona Scotti/IRSN.

The new seismic zoning of France for conventional buildings (and Installations Classified for Environmental Protection[438]), which came into force on 1 May 2011, is based on a probabilistic assessment of seismic risk; however, it was established using shorter earthquake return periods than those required for nuclear facilities (more than 10,000 years).

▶ Recommendations adopted at international level

Four extra-statutory regulations are used as a reference in France for taking into account seismic risks:

- RFS 2001-01 (2001), Determination of the Seismic Risk for the Safety of Surface Basic Nuclear Installations (*Détermination du risque sismique pour la sûreté des*

[438] *Installation classée pour la protection de l'environnement* (ICPE).

installations nucléaires de base de surface), which replaced RFS I.2.c (1981), Determination of the Seismic Movements to be Taken into Account for Installation Safety (*Détermination des mouvements sismiques à prendre en compte pour la sûreté des installations*);

- RFS I.3.b (1984), Seismic Instrumentation (*Instrumentation sismique*);
- ASN Guide 2/01 (2006), Taking into Account Seismic Risk in the Design of Civil Works at Basic Nuclear Installations, Excluding Facilities for the Long-Term Disposal of Radioactive Waste (*Prise en compte du risque sismique à la conception des ouvrages de génie civil d'installations nucléaires de base, à l'exception des stockages à long terme des déchets radioactifs*), which replaced RFS V.2.g (1985), Seismic Calculations for Civil Works (*Calculs sismiques des ouvrages de génie civil*);
- RFS I.3.c (1985), Geological and Geotechnical Site Studies; Determination of Soil Characteristics and Study of Soil Behaviour (*Études géologiques et géotechniques du site ; détermination des caractéristiques des sols et études du comportement des terrains*).

RFS I.3.c contains several recommendations pertaining to study of the following:

- the risk of soil 'liquefaction'[439], which can occur during high-intensity earthquakes; the results of the study must demonstrate that there is a sufficient safety margin with regard to the risks of propagation of liquefaction in the relevant soil layers and in any backfill;
- the stability of slopes (earth, rock, etc.), whether natural or man-made;
- the risk of recurrent faulting[440]: if soil surveys on the site reveal irregular contact surfaces that could be interpreted as manifestations of a fault, detailed tectonic analyses must be carried out to ensure that the risk of recurrent faulting can be ruled out throughout the facility lifetime. This forms part of the study on fault displacements at the source of seismic risks, known as 'capable faults', i.e. the study of active faults characterized as having significant potential to produce movement at the ground surface.

For earthquakes, ASN Guide No. 22 sets out two safety objectives:

- "In the event of an earthquake considered as a design extension condition, the reactor core (especially the structure of the fuel assemblies), the vessel internals and the control rod drive mechanisms must be capable of achieving reactor shutdown, while keeping the reactor in a subcritical state and sustaining fuel cooling."

[439] A process in which the behaviour of a substance changes to become like that of a liquid. For sand, liquefaction corresponds to a total temporary or permanent loss of shear strength. It is a common phenomenon. The most iconic images are those of the Niigata earthquake in Japan in 1964, the Christchurch earthquake in New Zealand in 2011 and, more recently, in 2018, the Palu earthquake in Indonesia.

[440] Movement of the contact surfaces (created by cracks) of a fault in relation to each other.

- “Structural elements must be strong enough to ensure that the spent fuel pool remains capable of performing its safety functions under earthquake conditions considered as a design extension condition.”

At international level, two documents are worthy of particular mention:

- IAEA Standard NS-R-3, published in 2003 and revised in 2016, entitled Site Evaluation for Nuclear Installations;
- the WENRA guide dated 11 October 2016 entitled Guidance Document Issue T: Natural Hazards/Guidance on Seismic Events/Annex to the Guidance Head Document on Natural Hazards.

Standard NS-R-3 emphasizes the importance, when choosing a site for a nuclear facility, of assessing the risk of faults on the ground surface[441] at the site, through an investigation of capable faults based on the best geophysical, geomorphological, geodesic and seismological knowledge available. If this investigation shows that a capable fault exists that could affect facility safety, an alternative site should be found.

The WENRA guide provides further explanations regarding earthquakes, in addition to the general document on ‘reference levels’ (for nuclear power reactors) applicable to natural hazards, which was updated in light of lessons learned from the Fukushima Daiichi nuclear power plant accident[442]. It provides a non-exhaustive list containing several points to be examined:

- the possible existence of site effects and capable faults;
- the different kinds of phenomena that could result from an earthquake (instabilities, dynamic soil compaction or soil liquefaction, fire, floods, failure of dams, loss of off-site power, consequences of failures at nearby industrial facilities initiated by an earthquake, etc.);
- how deterministic approaches (DHSA[443]) and probabilistic approaches (PSHA) can be used in studies aimed at defining the ground motions to be taken into account in the design basis of the facility or in the design extension conditions;
- how to determine the maximum ground motion to be used in the design basis of the facility, which must be based on reliable geological, seismological, paleoseismological and geotechnical data; ‘maximum credible earthquakes’ (MCEs) should be determined based on the properties of relevant faults;
- in the design extension conditions, earthquakes with a frequency of occurrence of less than 10^{-4} per year should be studied, including adequate margins to take into account uncertainty; an assessment of the margins and the risk of cliff-edge effects should be carried out by analysing the robustness of the equipment that ensures fundamental safety functions.

[441] Surface faulting.

[442] WENRA, 2014. Guidance Document Issue T: Natural Hazards.

[443] Deterministic Seismic Hazard Analysis.

12.4. External floods

It seems almost paradoxical that flooding at a nuclear power plant could cause serious cooling problems in the plant reactors. However, this is actually the case. In the absence of appropriate measures, the reactors could, through submersion or mechanical destruction, lose the on-site and off-site power supplies they need to drive coolant pumps and other systems (even those with a turbine) that can ensure cooling for a certain length of time. The (partial) flooding of the Le Blayais nuclear power plant site in late 1999 and the submersion of the Fukushima Daiichi nuclear power plant in March 2011 by a tsunami, although different in scale, both revealed the effects and damage that external floods can cause to important components in nuclear reactors (see chapters 24 and 36).

The treatment of flood risk at nuclear sites caused by river floods or rises in sea level (in the case of river or coastal sites), is discussed in greater detail below, though other phenomena (such as local rainfall) must also be taken into account when choosing sites and designing reactors.

▶ Approach used for the construction of French nuclear power reactors to address external flood risk

EDF at first decided to protect each of its nuclear power plants from external floods considered as plausible by selecting an appropriate site platform elevation. The method for determining the site platform elevation was different for each type of site.

For the 900 MWe reactor sites, the following method was used:

– for river sites, the highest of the following levels was used:
  - the level of an estimated 1000-year flood;
  - the level caused by the highest known flood, or the 100-year flood if higher, combined with the impact of destruction of the largest upstream water-retaining structure;

– for coastal sites, the height of the highest calculated high tide (tidal coefficient of 120) combined with the 1000-year storm surge was selected;

– for estuary sites, the highest of the following levels was used:
  - the level that could result from a combination of the 1000-year flood of the river and the tidal coefficient of 120,
  - the level that could result from a combination of the 100-year discharge flow rate, the upstream dam failure representing the highest potential hazard and the mean tidal coefficient of 70,
  - the level that could result from a combination of the 1000-year storm surge and the tidal coefficient of 120.

In all cases, the platform supporting items important to safety was set to an elevation at least equivalent to that determined using this method, and measures were taken to block water ingress channels below this level.

It became apparent that, at sites where the design-basis situation was the 1000-year flood, the probability of such a flood occurring (by definition around 10^{-3} per year) was high for a phenomenon likely to have significant consequences. In the opinion of the experts concerned, however, the idea that the discharge flow rate of a flood of much lower probability could be determined scientifically was unrealistic because there was no proven law in this area. The decision was therefore made to:

– take extra precautions in determining the water level resulting from the 1000-year flood. Whenever possible, uncertainties were estimated conservatively; the value chosen for the 1000-year flood discharge flow rate was not the calculated mean value, but the upper bound of the 70% confidence interval;

– add a 15% margin to the discharge flow rate.

The gain thus obtained could not be calculated and the safety organizations asked that measures be taken, as part of the on-site emergency plans, to provide protection against even greater floods. This approach was the subject of fundamental safety rule RFS I.2.e published in April 1984, defining a method for establishing the flood safety margin level, i.e. the water level likely to be reached at the site boundary, which was to serve as the basis for implementing appropriate protection.

Other phenomena that could cause flooding were taken into account on a case-by-case basis, using various approaches.

Since the flood monitoring system is capable of providing several hours' advance warning, it was accepted that a reactor could be brought to a safe shutdown state before the site platform was submerged.

Different methods of sealing entrances to buildings important to safety were studied and installed by EDF, particularly for the oldest nuclear power plants on the banks of the Loire, where the site platform design was based on the 1000-year flood, since there are no large dams on this river.

▶ From flooding at the Le Blayais nuclear power plant to the Flood Guide

Storm Martin, which swept southern France on 27 and 28 December 1999, caused extensive damage including flooding of part of the Le Blayais nuclear power plant site, entailing failure of systems important to safety. This event, described in Chapter 24, showed that the site protection measures, which were based on levels calculated using the methods recommended in RFS I.2.e, were insufficient, particularly for swell at an estuary site. It was waves generated by the storm in the Gironde estuary that had breached the protective dykes around the Le Blayais nuclear power plant.

This event led to the installation of reinforced flood protection at all relevant nuclear sites from 2000 (until 2014), as described in Chapter 24. Reinforced protection measures involved mainly implementation of the 'watertight volume' approach and also included increasing the height of certain dykes. For the Flamanville 3 EPR, the site platform was raised 4 m above the flood safety margin level.

In parallel, the French Nuclear Safety Authority (ASN) decided to revise RFS I.2.e to systematically take into account all phenomena that could cause flooding of a nuclear facility (illustrated in the schematic diagram in Figure 12.6).

Work to update RFS I.2.e – based mainly on experience feedback from the flood at the Le Blayais nuclear power plant site in 1999 – began with the involvement of several organizations (including EDF, Areva and IRSN as lead) that set out to examine the risks of all kinds of external floods, with studies on the applicability of statistical methods to explain events qualified as outliers[444], and other subjects such as extreme rainfall, the treatment of heterogeneity in statistical data processing (particularly data on river floods), the historical analysis of exceptional events (such as tsunamis on the Atlantic coast) and risk assessment of percolation through dykes[445]. Eight phenomena were taken into account in addition to the five covered by the 1984 fundamental safety rule.

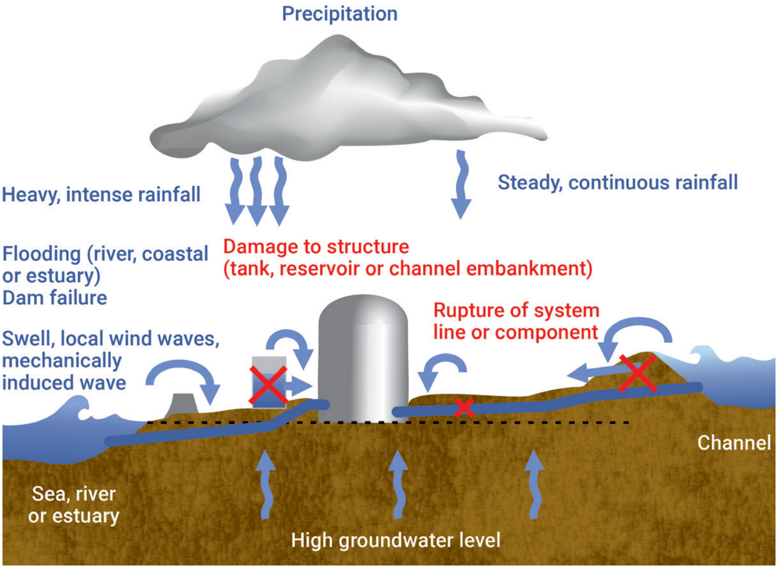

Precipitation
Heavy, intense rainfall
Steady, continuous rainfall
Flooding (river, coastal or estuary)
Dam failure
Damage to structure (tank, reservoir or channel embankment)
Rupture of system line or component
Swell, local wind waves, mechanically induced wave
Channel
Sea, river or estuary
High groundwater level

Figure 12.6. Simplified diagram showing the different phenomena that can cause flooding at a nuclear power plant site and the possible consequences. Georges Goué/IRSN.

[444] In statistics, an outlier is an observation with a value that differs significantly from that of most other observations in the same data sample.

[445] The findings are presented in the publication *L'aléa inondation – État de l'art préalable à l'élaboration du guide inondation pour les installations nucléaires* (Floods – State of the Art Prior to Preparation of the Flood Guide for Nuclear Facilities), IRSN, *Avis et rapports/rapports d'expertise/sûreté nucléaire* series, 2013.

For each phenomenon (sea level and associated events – including tsunamis –, river floods and associated phenomena, phenomena that can affect all types of sites [rain and water run-off, high groundwater levels, dam failures]), the following were examined:

- basic data,
- physical parameters to be quantified (intensity, volume, water level, etc.),
- existing characterization methods (deterministic or statistical), with identification of their limitations,
- identification and incorporation of uncertainties,
- the influence of climate change,
- interdependence between the different phenomena or events.

This led to the publication in 2013 of ASN Guide No. 13[446] (the Flood Guide), written for facility operators, providing recommendations on the assessment and quantification of external flood risks, and the definition of adequate means of protection against them, considering a wide variety of situations that can arise from a flood: site inaccessibility (impassable roads), unavailability of support functions (such as off-site power supplies, water intake [clogged by debris] and external emergency response teams), simultaneous damage to several facilities on a site, etc. As stated earlier, the guide was produced in the wake of lessons learned from the Le Blayais nuclear power plant flood in late 1999. Aside from these direct lessons, the review of the state of the art gave rise to in-depth reflection based on more advanced knowledge to ensure that external flood risks were taken into account more comprehensively and more robustly. ASN Guide No. 13 constitutes a reference text not only for new nuclear facilities being planned, but also for the ten-yearly reassessments of units in operation.

The recommendations in ASN Guide No. 13 state that 'reference flood situations'[447] should be defined based on events or combinations of events whose characteristics may be increased if necessary (by establishing the most unfavourable combinations or applying margins to compensate for the limits of current knowledge). Combinations of events are chosen where there is a proven or presumed dependency between events likely to cause flooding. In addition, when the potential for concomitance has been identified, in light of the duration and frequency of any one of the events, their combination is to be taken into account.

The ASN guide lists the different reference flood situations to be taken into account:

[446] ASN Guide No. 13, Protection of Basic Nuclear Installations Against External Flooding, 8 January 2013.

[447] External flood risk differs from other external hazards because of the diversity of phenomena to be taken into account. Because of this diversity, it is not always easy to determine extreme events. The working group sought to define reference flood situations for which the exceedance probability would be 10^{-4} per year, taking into account uncertainties. However, recommendations in the guide do not make explicit reference to an exceedance probability value.

- **for all sites, at least the following five reference flood situations:**
    - local rainfall;
    - small watershed flooding;
    - deterioration or failure of structures or equipment;
    - mechanically induced wave[448];
    - high groundwater level;
- **for all river sites:**
    - large watershed flood: the reference flow rate corresponds to the peak flow rate associated with the 1000-year return period flood, with the upper bound of the confidence interval set to 70%, increased by 15%;
    - failure of a water-retaining structure: the scenario to be considered is failure of the water-retaining structure that would lead to the most severe potential consequences for the site;
    - local wind waves[449];
- **for coastal sites:**
    - tides: the maximum level of the theoretical tide is combined with the 1000-year return period storm surge (with the upper bound of the confidence interval set to 70%), increased to take into account uncertainties associated with the evaluation of rare storm surges (outliers);
    - waves (ocean waves and local wind waves);
    - seiches[450];
    - tsunamis, etc.

The ASN guide also gives special consideration to estuary sites.

Operators of nuclear facilities must obviously monitor changes in the flood risks at their site and take measures to acquire qualitative and quantitative data for this purpose throughout the operational lifetime of the facility.

[448] A mechanically induced wave is a wave travelling along the open surface of water in a channel, induced by a sudden variation in the speed (flow rate) of the flow. This phenomenon is similar to 'hammering' that can occur in pipes. A mechanically induced wave can be observed during the sudden stopping or starting of the generators at a run-of-river hydroelectric power plant, or of the raw water system pumps in an open-circuit water intake channel of a nuclear power plant.

[449] Effect of wind on the surface of the water.

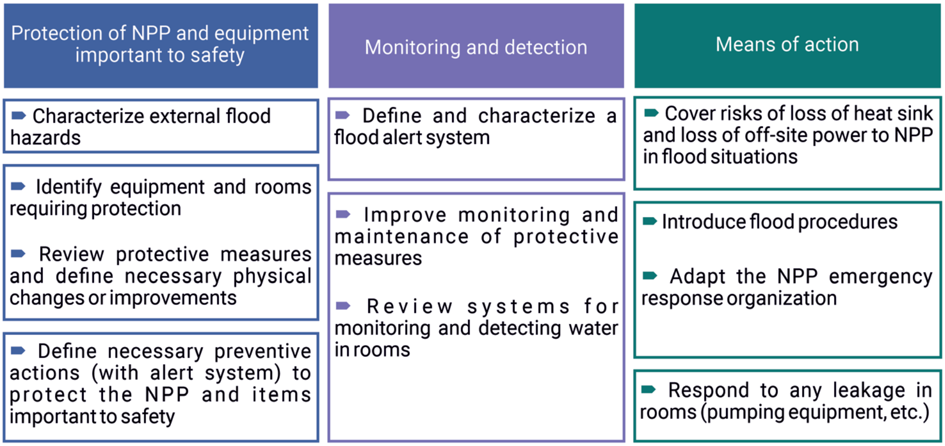
[450] A seiche is a stationary wave that can occur in a closed or semi-closed area of water such as a harbour, pond, lake or bay. In a semi-closed maritime dock, seiches are caused by the penetration of long waves from the open sea. Seiches usually have a period of between two minutes and a few tens of minutes. If the period of the seiche coincides with the resonance period of the dock, it can be amplified by resonance inside the dock. This motion can continue for a few minutes, a few hours or even several days, even when the initiating phenomenon has disappeared.

ASN Guide No. 13 presents several recommendations on methods for assessing, on a nuclear facility site, the consequences of the various phenomena listed above as well as the organizational and physical protective measures that can be implemented to ensure continued compliance with fundamental safety rules. These measures must aim to provide several 'lines of defence' that are as independent as reasonably possible. The guide also recommends assessment of the risk of a cliff-edge effect for each reference flood situation.

The guide mentions cases where facility protection measures against a reference flood situation are based partly on an alert system, a subject developed in greater detail below.

▶ Management of flood alert situations

Among the many safety issues raised by the partial flooding of the Le Blayais nuclear power plant, two subjects that were examined concerned monitoring flood risks at nuclear power plant sites and management of alert situations. The diagram in Figure 12.7 shows how the various issues relate to one another.



Protection of NPP and equipment important to safety

- Characterize external flood hazards
- Identify equipment and rooms requiring protection
- Review protective measures and define necessary physical changes or improvements
- Define necessary preventive actions (with alert system) to protect the NPP and items important to safety

Monitoring and detection

- Define and characterize a flood alert system
- Improve monitoring and maintenance of protective measures
- Review systems for monitoring and detecting water in rooms

Means of action

- Cover risks of loss of heat sink and loss of off-site power to NPP in flood situations
- Introduce flood procedures
- Adapt the NPP emergency response organization
- Respond to any leakage in rooms (pumping equipment, etc.)

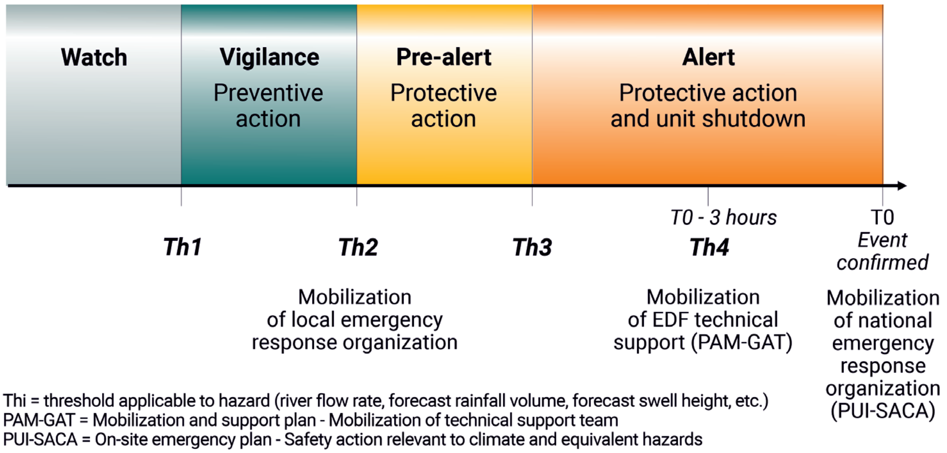
Figure 12.7. Diagram showing the different issues examined following flooding of the Le Blayais nuclear power plant. IRSN.

Where it has been considered appropriate, a flood alert system has been set up for predictable external floods (particularly river or coastal floods and heavy rain) so that early action can be taken to protect sites (for example, by closing passageways through a dyke, checking that watertight volumes are sealed, monitoring the pumping station and bringing reactors to a safe shutdown state) and bring in the human resources and equipment required if the site were to be temporarily isolated.

The need for this type of alert system and defining the system specifications (timing of alerts, number of phases) depend on site vulnerability to various external flood phenomena, especially with regard to the following risks:

- risk of flooding at the nuclear island platform elevation;
- risk of site isolation (making it inaccessible),
- risk of loss of off-site power to the facility reactors,
- risk of impairment of the water intake filtration function (for the heat sink) due to debris displaced by floodwater, potentially compromising the ability of reactors to pump the water they need.

This alert system must be closely linked with special flood procedures that stipulate the required course of action to be taken on site prior to and during the flood. It must give sufficient advance warning and may have up to four graduated phases, as shown in the diagram in Figure 12.8 below: watch (normal operation), vigilance (preventive action), pre-alert (additional action) and alert (reactors brought to a safe shutdown state).


Watch
Vigilance
Preventive action
Pre-alert
Protective action
Alert
Protective action and unit shutdown
Th1
Th2
Th3
T0 - 3 hours
Th4
T0
Event confirmed
Mobilization of local emergency response organization
Mobilization of EDF technical support (PAM-GAT)
Mobilization of national emergency response organization (PUI-SACA)

Thi = threshold applicable to hazard (river flow rate, forecast rainfall volume, forecast swell height, etc.)
PAM-GAT = Mobilization and support plan - Mobilization of technical support team
PUI-SACA = On-site emergency plan - Safety action relevant to climate and equivalent hazards

Figure 12.8. Diagram showing the phases of the flood alert system for a nuclear power plant site. IRSN.

Emergency response must also be organized to take into account the specific characteristics of external floods: all the reactors on a site may be simultaneously affected and the site may find itself isolated (making it difficult to bring in response teams and equipment). The alert phase leads to implementation of the 'on-site emergency plan', or calling on the national emergency response organization involving EDF, ASN, the prefect(s) concerned, IRSN and others, these measures being subsequent to on-site emergency response procedures initiated in the pre-alert phase.

▶ Lessons learned from the Fukushima Daiichi nuclear power plant accident regarding external flood hazards

As for seismic risks, the accident in March 2011 at the Fukushima Daiichi nuclear power plant raised questions about the risks of higher external floods than those used in the design basis for nuclear power reactors, which could simultaneously affect all units on a single site (see Chapter 36).

The measures implemented for nuclear power reactors following the complementary safety assessments are based on the concept of a 'hardened safety core' of equipment capable of withstanding more large-scale external floods than the those initially taken into account in designing protective measures for the facility.

– **Sea level:**

  At the Le Blayais and Gravelines sites, EDF followed the recommendations of ASN Guide No. 13, adding a fixed margin of 50 cm to the sea level corresponding to the maximum theoretical tide combined with a 1000-year storm surge when defining protection for the hardened safety core equipment. To calculate the 1000-year storm surge, a statistical approach was taken based on regional and historical information. Certain aspects (taking into consideration outliers, for example) were examined in greater detail in research and development work, while at the same time meeting the schedule for deployment of the planned protective measures for hardened safety core equipment on both sites.

– **River level:**

  For the river level, EDF added a 30% margin to the reference river flood to protect the hardened safety core equipment, particularly in view of the behaviour of hydraulic civil works at these flood levels.

– **Rain and floods caused by an earthquake:**

  To protect the hardened safety core equipment, EDF used three scenarios in which water falls directly onto the site platform: 100-year rainfall doubled, 100-year rainfall combined with total blocking of the rainwater drainage system and flooding caused by failure of structures or equipment on the site due to a 'hardened safety core' earthquake. Decoupling values were chosen by EDF to design protection for the hardened safety core equipment on each site, adding a margin that varied according to each site in function of the calculated maximum water depth.

▶ Recommendations and requirements adopted at international level

As explained above, in France, taking into account flood risk at nuclear facilities was covered in fundamental safety rule RFS I.2.e (1984), *Prise en compte du risque d'inondation d'origine externe* (Taking into Account Flood Risk from External Sources), which was replaced by ASN Guide No. 13 (2013), Protection of Basic Nuclear Installations Against External Flooding.

More recent recommendations were set out in ASN Guide No. 22, which were explained in Section 12.1. Those that are general in scope obviously apply to flood risks from external sources.

At international level, the following documents are worthy of mention:

- Standard NS-R-3 of the IAEA, published in 2003 and revised in 2016, entitled Site Evaluation for Nuclear Installations, described previously in Section 12.3;
- WENRA guide dated 11 October 2016, entitled Guidance Document Issue T: Natural Hazards/Guidance on External Flooding/Annex to the Guidance Head Document on Natural Hazards.

The WENRA guide provides further explanations on external flooding, to supplement the general document on 'reference levels' for natural hazards, which was updated in light of lessons learned from the Fukushima Daiichi nuclear power plant accident[451]. This guide:

- lists the large number of phenomena that can ultimately lead directly or indirectly to flooding at a nuclear facility site (including landslides, snow or glacier melt);
- emphasizes, as in the case of earthquakes, the need to take into account hazards that could plausibly be combined with external floods and the induced effects of external floods;
- for studies on facility protection, the guide specifies several phenomena likely to occur at the site due to flooding, consequently compromising the operation of equipment that performs safety functions (through pipe congestion, clogging of pipes or outlets by debris, inaccessibility to the facility site or buildings, etc.);
- as in the case of earthquakes, provides information on how to determine the parameters used in the design basis of a facility (such as water height and water flow rate), which must take into account the widest and most reliable historical data available and, to prepare for the future, must also take into account, as necessary, expected changes in the climate during the planned lifetime of the facility;
- recommends, in the design extension conditions, taking into account external floods with a frequency of less than 10^{-4} per year, incorporating adequate margins to include uncertainty; the margins and risks due to cliff-edge effects should be assessed by conducting a sensitivity analysis of the factors influencing flood characteristics, to assess the vulnerability of equipment performing the fundamental safety functions in external flood situations.

12.5. Extreme temperatures

12.5.1. Extreme cold

Pressurized water reactors in the 900 MWe and 1300 MWe range are designed to operate in cold weather, at a design temperature of -15°C (considered as unlimited in time). There was no particular procedure at the time of their design for taking into account lower temperatures corresponding to extreme cold.

[451] WENRA, 2014. Guidance Document Issue T: Natural Hazards.

During the very cold winters of 1985-1986 and 1986-1987, a number of events occurred in France caused by freezing (leading in particular to malfunctions on measuring devices located outdoors). EDF established a nationwide extreme cold procedure to ensure electrical power generation could continue under satisfactory safety conditions. It aims to enable facilities to withstand much lower temperatures than the design temperature (for up to 6 h and down to -33°C at certain sites). It was applied to 1450 MWe reactors and the EPR from the design stage, and implemented for the 900 MWe and 1300 MWe units during their periodic reviews. Studies by EDF led to several equipment changes (installation of extra heating, reduction of ventilation rates in some buildings, better cold protection for pumping station equipment, etc.) as well as organizational changes (operating instructions for extreme cold conditions, applicable from October until April of the following year) for units in service.

However, it appears necessary to keep a careful watch on any changes in the climate. EDF's climate watch, described in Section 12.2, is a valuable contribution to studies associated with safety reassessments, especially those for the fourth ten-yearly inspections conducted on 900 MWe units.

12.5.2. Extreme heat

During the summer heatwaves in 2003 and 2006 (and, more recently, in 2015 and 2019), the temperatures recorded at some sites exceeded the temperatures used to design the reactors at the nuclear power plants in operation. Like the procedure for extreme cold, EDF developed a nationwide extreme heat procedure to ensure electrical power generation could continue during a heatwave under satisfactory safety conditions. As part of this work, EDF checked that the maximum air and heat sink temperatures[452] likely to be recorded up to 2030 would not affect availability nor impair operation of the equipment necessary to bring reactors to a safe shutdown state and to mitigate any radiological risks. In some cases, potential improvements were identified to ensure that equipment would perform correctly. EDF then made some physical and organizational changes to both design and operation, for example:

- thermal protection of water reserves,
- improved performance of the heat exchangers used to cool certain items important to safety,
- replacement and improved performance of certain air conditioning units,
- introduction of shutdown procedures for equipment items not important to safety where continued operation could raise the temperature inside buildings,
- changes to operating procedures to prevent overheating on items important to safety.

[452] Up to 45.9°C for the instantaneous air temperature at the Golfech site and up to 36°C for the instantaneous heat sink temperature at the Dampierre-en-Burly site.

The approach for the EPR differs in that the maximum temperatures likely to be observed up to the end of the 21st century (maximum instantaneous air temperature of 42°C at the Flamanville site) were taken into account in facility design (in buildings, ventilation systems and others).

As in the case of extreme cold events, EDF's climate watch contributes significantly to studies associated with safety reassessments, especially those for the fourth ten-yearly inspections conducted on 900 MWe units.

Finally, it should be noted[453] that the water taken from rivers or the sea to cool reactors is generally discharged at a higher temperature, either directly or after being cooled in cooling towers, so that some of the heat is discharged into the atmosphere.

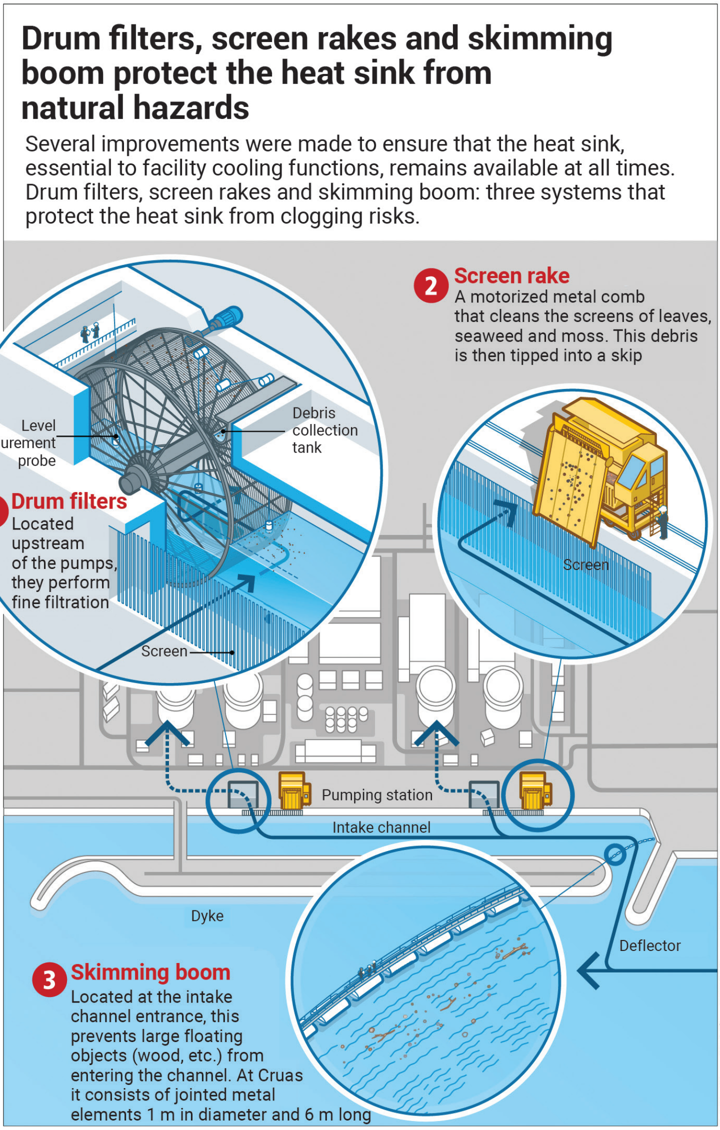
For nuclear power plants using river water, the French Nuclear Safety Authority (ASN) has placed conditions at each site on the discharge of water used for cooling. To protect the environment, especially the ecosystem, limits are set on temperature rises in streams and rivers due to nuclear power plant operation, including the water temperature downstream of plants. If these limits are exceeded, the operator must reduce reactor power or shut down the reactor. A temporary relaxation of the temperature limits on heated discharges may be authorized by the ASN when the power grid so requires, as was the case during the 2003 and 2006 heatwaves. Environmental monitoring is reinforced in this case.

12.6. Possible heat sink hazards

The nuclear fuel in the reactor core (whether the reactor is in operation or shut down) and in the spent fuel pool needs to be cooled constantly. A heat sink is required for this purpose. The heat sink is generally water from the sea or a river, depending on the plant's geographical location. Water is taken from the natural environment at a pumping station, which filters it in a two-stage filtration process (pre-filtration followed by fine filtration – see Figure 12.9). Pumps circulate the water to heat exchangers, where it heats up before being discharged into the natural environment. The water level and flow rate at the pumping station must be high enough to allow pumps to operate correctly.

Because it is at the interface with the natural environment, the pumping station, which contains the equipment required to filter and circulate water, is particularly exposed to climate and environmental conditions. Blockage of the water intake or a significant increase in head loss in filtration devices can have major consequences for reactor safety. This is referred to as 'heat-sink clogging'. Measures are taken both to avoid clogging and to mitigate risks if it occurs.

[453] This does not affect nuclear reactor design, but is worth mentioning (see the ASN website).



Drum filters, screen rakes and skimming boom protect the heat sink from natural hazards

Several improvements were made to ensure that the heat sink, essential to facility cooling functions, remains available at all times. Drum filters, screen rakes and skimming boom: three systems that protect the heat sink from clogging risks.

1 Drum filters
Located upstream of the pumps, they perform fine filtration

2 Screen rake
A motorized metal comb that cleans the screens of leaves, seaweed and moss. This debris is then tipped into a skip

3 Skimming boom
Located at the intake channel entrance, this prevents large floating objects (wood, etc.) from entering the channel. At Cruas it consists of jointed metal elements 1 m in diameter and 6 m long

Antoine Dagan/Spécifique/IRSN - Source : IRSN/Magazine *Repères*

Figure 12.9. Diagram showing the various devices protecting nuclear reactor heat sinks against the risks of clogging.

Over the many years of NPP operation accumulated in France and other countries, there have been numerous events affecting nuclear power reactor heat sinks. The most significant recent events in France in terms of consequences for safety are:

- sand build-up in the intake channel at the Chinon nuclear power plant, observed in December 2005,

- freeze-up of the water intake at the Chooz B nuclear power plant on 9 January 2009[454],
- total clogging of the heat sink at the Cruas-Meysse nuclear power plant on 1 December 2009[455].

Clogging agents can be of various origin: plant (such as seaweed), animal (small fish, among others), mineral (frazil ice) or man-made (petroleum products); this depends on the environment and therefore can vary from one facility to another. Depending on their size, clogging agents affect different filtration stages at variable rates: if they are large, they accumulate on the water intake screens, which usually happens slowly; smaller clogging agents affect the fine filtration stages and tend to accumulate more quickly. The finest particles pass through the filtration equipment and clog the heat exchangers, degrading their heat exchange capabilities.

Frazil ice is an ice crystal formation that occurs in water under extreme cold conditions (see Figure 12.10). The water stays in liquid form in a thermodynamically

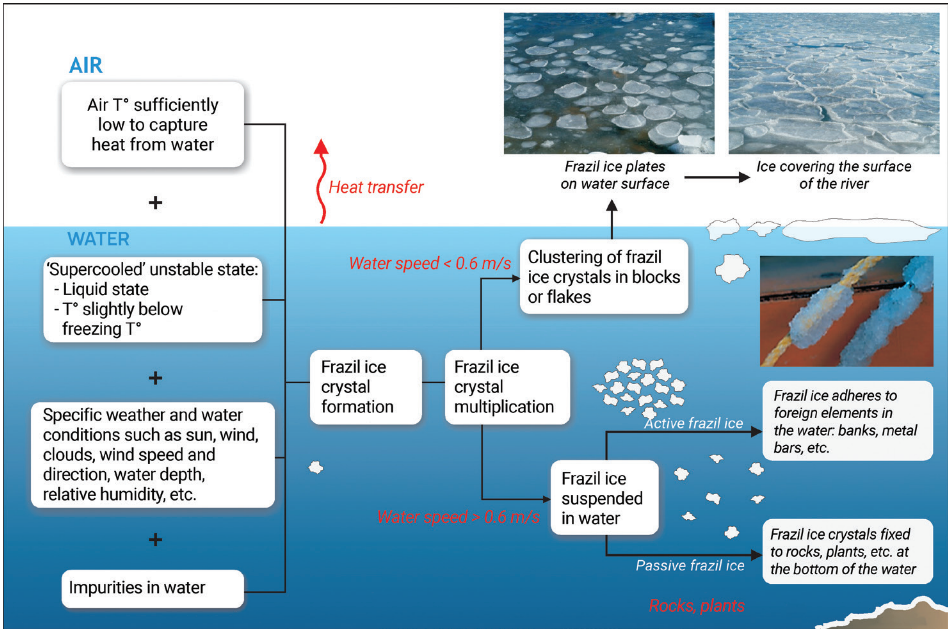

AIR
Air T° sufficiently low to capture heat from water
+
Heat transfer
Frazil ice plates on water surface
Ice covering the surface of the river
WATER
'Supercooled' unstable state:
- Liquid state
- T° slightly below freezing T°
Water speed < 0.6 m/s
Clustering of frazil ice crystals in blocks or flakes
+
Frazil ice crystal formation
Frazil ice crystal multiplication
Specific weather and water conditions such as sun, wind, clouds, wind speed and direction, water depth, relative humidity, etc.
Active frazil ice
Frazil ice adheres to foreign elements in the water: banks, metal bars, etc.
Frazil ice suspended in water
Water speed > 0.6 m/s
+
Frazil ice crystals fixed to rocks, plants, etc. at the bottom of the water
Passive frazil ice
Impurities in water
Rocks, plants

Figure 12.10. Frazil ice formation and development in a river. Georges Goué/IRSN Media library.

[454] Overnight on 9 January 2009, the temperature of the Meuse fell below zero. Ice blocked the anti-intrusion grille upstream of the plant's pumping station. In the morning, the water level fell by two metres in the channel supplying the reactor heat sink, threatening the water supply to the pumps.

[455] Early in the evening on 1 December 2009, around 50 tonnes of plant matter collected on the screens at the pumping station of units 3 and 4 at the Cruas-Meysse plant (Ardèche). There was a total loss of heat sink for Unit 4, which had to be shut down.

unstable state, even though its temperature is slightly below the freezing temperature of water. Depending on conditions, the ice crystals form clusters when they encounter obstacles or migrate to the water surface.

A massive build-up of clogging agents is said to occur when the affected reactor is forced to stop power generation: the pumps used to circulate the cooling water essential for generating electricity, known as 'production pumps', are shut down.

A massive build-up of clogging agents is a hazard that regularly affects French nuclear power plants: approximately 80 clogging events were recorded between 1979 and 2013. This number should not mask the great disparity between sites: at some facilities (Belleville-sur-Loire, Nogent-sur-Seine, Saint-Alban, Saint-Laurent-des-Eaux B and Cattenom), massive clogging has never been recorded, whereas at others, such as Le Blayais and Paluel, these events occur regularly.

Alert systems provide graduated monitoring of heat sinks during periods of risk or when a massive build-up of clogging agents is imminent. However, at present, the main strategy used to avoid a massive build-up of clogging agents is to significantly decrease the flow of water to the pumping station in order to reduce the rate of clogging on screens or filters and of head loss through the filtration equipment, so as to maintain a long-term flow that is compatible with the cooling of items important to safety. To achieve this state, the operator shuts down the production pumps. Following the event at Cruas in 2009, EDF enhanced existing measures by introducing water level measurement at all pumping stations, combined with automatic pump shutdown on detection of a low water level, all provided in a special interface for control room operators.

To address the other hazards affecting the heat sink, EDF uses monitoring and other appropriate measures; for example:

– at nuclear power plants where frazil ice risk has been identified, monitoring is performed according to a special operating rule. Physical changes have also been made, such as recirculation in winter, which brings hot water to the pre-filtration stage in the pumping station;

– changes in river levels are monitored daily and there are agreements in place with the operators of water-retaining structures to adjust the flow in these rivers so that they remain at a level compatible with the safety of the nuclear facilities on their banks;

– regular bathymetric measurements of the natural environment up to the water intakes to detect sand and/or silt build-up on intake channels and begin dredging, if necessary.

Regardless of the circumstances, accident situations corresponding to loss of water supply to the heat sink are always studied as part of the reactor safety demonstration (see Chapter 13 on the complementary domain).

12.7. Other naturally-occurring external hazards

To take into account strong winds and snow, the designers of civil works use snow and wind rules that are not specific to nuclear facilities. The loads considered are significant, but frequency rates are not as low as the values mentioned earlier for other external hazards, because available statistical data is limited. Designers may also add extra safety margins, depending on the importance of what is being protected. Since the early 2000s, Eurocodes (final version) have also been used.

12.8. Accidental aeroplane crashes (excluding malicious acts)

There is not much in common between the light aircraft flown by amateur pilots and the jumbo jets used in commercial aviation. Air traffic is also not the same throughout France, and the phases of a flight in which accidents occur most often are take-off and landing. There is therefore no single way to manage this risk. There are, however, vast amounts of data for this activity. Historically this has meant that a statistical approach to this risk and its assessment is possible, particularly during the design of French nuclear reactors, which is presented only briefly here.

▶ Approach used historically for nuclear power reactors

Three groups of aircraft have been identified:

- the first group consists of commercial aircraft, i.e. passenger and freight planes, as well as mail planes; all civil aircraft weighing more than 5.7 t belong to this category;
- the second group consists of military aircraft;
- the third group covers general aviation aircraft (weighing less than 5.7 t).

Statistical data was available to calculate estimated annual averages for crashes in France: one commercial aircraft, several military aircraft, and several hundred light aircraft. For the three types of aviation, it was assumed that probability calculations could be divided into three parts: a large part for landing, roughly one third for aircraft in flight, and a small part for take-off. For a facility located outside of an airport approach zone or take-off zone, the probability could therefore be divided by 3.

This meant that it was possible to determine the average annual probability for aeroplane crashes outside airport zones throughout France, and then, taking into account the virtual surface area of nuclear facilities, to calculate the annual probability of a crash on these facilities. Probability has been estimated at approximately 10^{-8} for commercial aviation, 10^{-7} for military aviation and a few 10^{-6} for general aviation.

These values are usually conservative: they do not take into account any bans on overflight that may be in place, nor the fact that in many accidents it is possible to avoid certain points of impact.

With probabilities available for aeroplane crashes, it is possible to determine the associated risks on the basis that, if no particular protection is in place, all the equipment in an affected building will be destroyed, which is also a conservative assumption.

The fundamental safety rule on the risks of aeroplane crashes (RFS I.2.a), published in August 1980, gives the following indications:

- "the (logarithmic) order of magnitude of the limit probability for acceptance of an unacceptable release of radioactive substances at the site boundary, for each of the safety functions, is 10^{-6} per year per reactor;
- however, to take into account the necessary summation of probabilities of accidents with similar consequences, for each hazard family a limit of 10^{-7} per year per reactor is set for the order of magnitude of the probability of the event, for each of the safety functions."

Release of radioactive substances is assessed by taking into account the following three possible 'targets':

- the reactor itself; studies must confirm that the impact of the aeroplane in question would not result in unavailability of the fundamental safety functions;
- the spent fuel pool; studies must confirm, among other things, that the impact of the aeroplane would not cause spent fuel to melt (a possible decoupling criterion could be keeping spent fuel submerged);
- the treatment plant for radioactive effluent.

Given the characteristics of aircraft in circulation when the nuclear power plants were built and the different effects that impact could have on concrete structures, EDF chose the following two types of aircraft:

- a single-engine propeller aeroplane weighing 1500 kg, of which the 250 kg engine constitutes a 'hard', penetrating projectile: this was the CESSNA 210, which at the time represented approximately 80% of general aviation traffic;
- a twin-engine business jet weighing 5700 kg with the jets at the rear, which constitutes a 'soft' projectile causing widespread shaking throughout the affected building; this was the Learjet 23, which at the time represented approximately 20% of general aviation traffic.

An impact velocity of 100 m/s was considered, corresponding to a speed of 360 km/h.

As regards the resistance[456] of the buildings important to safety, including the reactor building, the impact of both types of aircraft was considered. Other buildings were only protected against the most probable 'perforating' impacts.

[456] Various phenomena that can be caused by an aeroplane impact must be examined, such as vibrations, perforation and scabbing, to name a few.

Many tests were carried out to develop and qualify the simulation software used in the studies.

Research into failure conditions, defined as elastic or plastic deformation of steels greater than 10%, has shown that, regardless of the point of impact on the reactor containment, the containment will resist the impact of an aeroplane weighing more than 13 t travelling at 150 m/s.

A site-by-site study of local air traffic conditions, reviewed periodically, was used to check that this standardized design basis was sufficient.

As part of the safety studies carried out in the framework of the fourth ten-yearly inspections of the 900 MWe units, EDF extended this approach to cover risks from helicopters.

Finally, the risks associated with the possible impact of a jumbo jet have been examined within a specific context, but will not be discussed further here.

▶ Measures taken for the EPR

One of the most significant measures taken for the EPR project as regards accidental aeroplane crashes is the adoption of an aeroplane crash (APC) shell to protect the reactor building, two of the four safeguard buildings and the fuel building. The APC shell has a very high reinforcement ratio and is also very thick.

The objectives and methods of studying aeroplane crashes are explained in detail in the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors:

- "measures must be taken to ensure adequate protection of safety-related buildings, with due consideration for general and military aviation traffic near the site and anticipating as far as possible how this will evolve during the lifetime of the plant";
- "protection of safety systems must be considered with regard to direct impact (penetration) as well as to indirect impact by induced vibrations";
- these objectives can be met "by the design of the reactor building, of the spent fuel building and some auxiliary buildings (so as to ensure without redundancy the protection of equipment needed to shut down the reactor and to prevent core melt)" using the two load/time diagrams, C1 and C2 (see Figure 12.11 below), applied to a circular area of 7 m^2:
    - diagram C1 is used to design the internal structures of these buildings so that they can withstand the induced vibrations; it is also used to design the external walls of the same buildings to withstand the loads resulting from a direct impact, so as to ensure that no penetration or scabbing occurs and any deformation (of rebars or concrete) remains limited;

- load/time diagram C2 is used for ultimate-limit-state design[457] (according to Eurocode 2, Part 1) of: the reactor building, to ensure perforation is avoided and that any scabbing that occurs does not compromise reactor operation or prevention of core melt; and the fuel building, to ensure spent fuel uncovery is prevented.

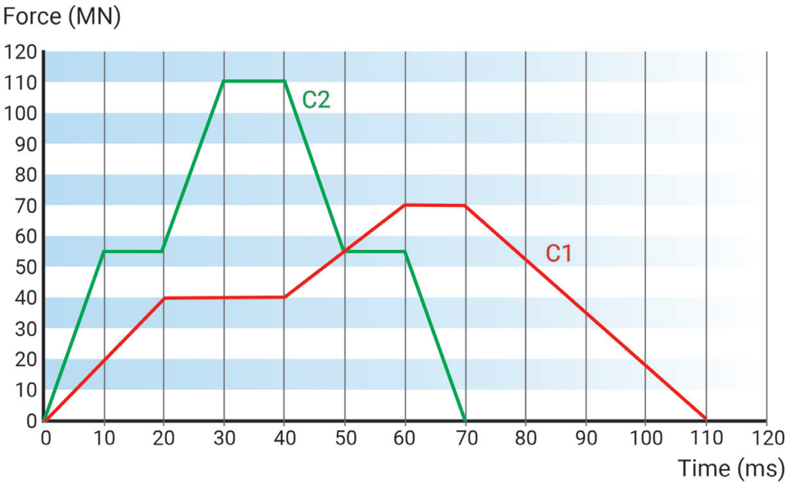


Figure 12.11. Aeroplane crashes: mechanical loading profiles taken into account for the EPR, in accordance with technical guidelines. IRSN.

▶ An evolving approach

The need to change the approach set out in RFS I.2.a emerged recently due to the following:

- probabilistic goals mean that accidental aeroplane crashes with very low probability but potentially very serious consequences are not taken into account – the Fukushima Daiichi nuclear power plant accident raised further questions about rare events with potentially very significant consequences. It should be noted that, in countries outside of France, for most new generation reactors, an aeroplane crash is considered independently with regard to the probability of this event;
- aviation is constantly changing (number of aircraft, traffic, flight management, etc.);
- taking into account induced effects (fires – including kerosene fires –, explosions, projectile emission, load dropping and others) is not explicitly mentioned in RFS I.2.a.

[457] The definition of the ultimate limit state in Eurocode 2, Part 1 is “the potential danger associated with the collapse of the structure or other forms of structural failure.”

In view of these considerations, IRSN has entered into technical discussions with EDF (particularly in the context of the safety reassessments associated with the third ten-yearly inspections of the 1300 MWe units) with a view to proposing a new approach for taking into account aeroplane crash risks.

12.9. Risks related to the industrial environment (excluding malicious acts)

The 'site description' chapter of safety analysis reports for basic nuclear installations has always presented a survey of the existing or planned industrial environment in an area of several kilometres around the facility. This does not necessarily lead to particular constraints on facility construction.

However, it rapidly became apparent that the problem deserved more detailed examination when the application for construction authorization for the Gravelines nuclear power plant was filed in 1975. The area near the site was heavily industrialized and in particular contained an oil depot where the nearest tanks were only 500 m from one of the reactors. The oil terminal supplying this depot provided berthing for very large ships at distances ranging from 1250 to 2000 m from the plant. Finally, because the Gravelines nuclear power plant was beside the sea, ships could run aground less than 650 m from the reactors, and explosion of the tanks on these ships had to be considered.

In addition, the Dunkirk Port Authority wanted to build a large liquefied natural gas (LNG) terminal and an LNG depot, which would lead to further risks. For example, if there was a collision between two ships, at least one of which contained LNG, some of the gas could spill, the cloud formed could drift and, if there was a conjunction of unfavourable conditions, the cloud could explode when it passed over the nuclear power plant. It was thus necessary to assess the potential consequences of this project with regard to facility safety and consider specific protective measures where necessary.

EDF therefore developed a method of risk assessment relevant to the industrial environment which focused particularly on explosion risks and followed the same line of reasoning as that applied to aeroplane crashes. The reference probability chosen was identical, i.e. 10^{-7} per year, per unit and per safety function, and a conservative approach was generally taken when considering the various uncertainties.

Based on the study, the authorities decided that the LNG terminal had to be built at least 4 km from the nuclear power plant and EDF chose to protect the buildings important to safety at the Gravelines facility so that they could withstand a triangular overpressure wave with an amplitude of 200 mbar and a duration of 300 ms, as well as radiation due to fire in the vicinity. Consequently, buildings and ventilation air intakes[458] were changed with regard to the reactor unit design used for the first

[458] To prevent an overpressure wave from penetrating the buildings.

programme contract and were reinforced accordingly. In addition, earth mounds were placed between the reactors and the oil tanks.

In 1982, fundamental safety rule RFS I.2.d was issued, pertaining to risks involved in industrial environments, transportation links (roads, railways, waterways) and pipelines, that could cause:

- a thermal hazard due to fire,
- an airborne pressure wave, an associated vibration wave and projectiles resulting from an explosion,
- a cloud produced by toxic, corrosive or flammable gases and smoke from a fire.

In this fundamental safety rule, a minimum design basis for nuclear facilities for an airborne overpressure wave (triangular in shape with a sharp front) is proposed (50 mbar peak, duration 300 ms). Plausible accident scenarios leading to anticipated hazardous phenomena must be analysed; the analysis must take into account any domino effects that could initiate another hazardous phenomenon, aggravating the effects of the first. Finally, a probability limit value for acceptance of an unacceptable release of radioactive substances at the site boundary was proposed (10^{-7} per year, per unit and per safety function for each hazard family).

With the publication of RFS I.2.d, the method for analysing industrial risks was adopted and applied systematically during preliminary reviews of the next series of reactors. Reactor design was checked to ensure it was adequate, taking into account not only stationary storage facilities, but also transportation involving trains, lorries, barges and other ships, as well as pipelines; the behaviour of openings and buildings was checked, and results showed that the other design constraints placed on structures and equipment guaranteed satisfactory resistance.

However, since the 1980s, hazardous phenomena such as the following have been identified or confirmed:

- in the case of flammable liquids, some products generate a particular form of boilover[459];
- in the case of flammable gases, the Buncefield accident in the UK in December 2005 confirmed the reality of and the danger posed by gas clouds (UVCEs[460]). The findings of hazard studies conducted to date show that this phenomenon was insufficiently described.

As a result of these developments, the operator of the crude oil depot neighbouring the Gravelines nuclear power plant updated their hazard study to take into account boilover risk. EDF analysed the impact of such an event and concluded that it would

[459] Boilover can happen when the surface of a liquid catches fire. If the heat generated by the flames reaches a layer of water at the bottom of the tank, it can cause this layer to vaporize instantly, projecting the burning oil out of the tank. The resulting eruption can be enormous.

[460] Unconfined Vapour Cloud Explosions.

lead to unacceptable failures of certain items important to safety. Discussions between EDF, the depot operator and the competent authorities resulted in a change of the product stored at the depot from crude oil to gas oil.

The foregoing illustrates the need – mentioned in the Order of 7 February 2012 (the INB Order) – to take prudent approaches to nuclear safety, using up-to-date, referenced data, along with appropriate, clearly explained and validated methods, while integrating appropriate assumptions and rules to suit the uncertainties and limits of knowledge pertaining to the phenomena involved, and implementing simulation software and models qualified for the relevant subject matter. Accident studies can be used to determine orders of magnitude for probabilities related to events that could lead to the hazardous phenomena studied when analysing industrial risks.

Chapter 13

Complementary Domain of Events

The previous chapters explained how nuclear power plant design and studies gradually came to include failures potentially resulting from internal or external hazards that were not sufficiently scrutinized when the type of water reactor was chosen and the first units were built. The introduction of probabilistic references to determine the acceptability of measures taken against certain risks, such as those related to turbines, aeroplanes, and external explosions, has also been covered in earlier chapters.

These changes have added supplements to the initial design basis without altering the most structured aspects, namely the study of internal events (incidents and accidents) in the form of operating conditions resulting from 'single' initiating events. These studies are conducted according to the approach described and illustrated in chapters 6 through 10. They were gradually supplemented by a 'complementary domain'[461] of events[462] (as well as core meltdown accidents which will be treated separately), covered in this chapter.

As indicated in Section 6.5, this complementary domain and the study of core-melt situations are now included (ASN Guide No. 22, WENRA texts) in what is known as the Design Extension Conditions (DEC). These conditions encompass equipment-related internal events (with category DEC-A for multiple equipment failures and category DEC-B for core-melt situations) as well as internal and external hazards that are more severe than those used for the conventional design basis.

[461] The French notion 'complementary domain' does not include severe accidents, unlike the notion 'design extension conditions' defined by the IAEA.

[462] The expression 'situations' is also used.

13.1. The origin of studies belonging to the complementary domain

In 1973, US nuclear safety organizations began posing questions on the possibility and potential consequences of a reactor trip (scram) failure during a transient leading to reactor trip, a situation known as ATWS (Anticipated Transient Without Scram). In all nuclear power plants, scram is a system that meets the single-failure criterion. After 1975, French nuclear safety organizations broadened the question and wanted Électricité de France (EDF) to study the probabilities and consequences of the complete failure of all systems important to safety that are permanently or frequently used, namely the electrical power supply, the heat sink and associated systems, and core cooling by the steam generators.

The electrical power supply necessary for maintaining safety included the two relatively independent off-site grids, the possibility of islanding if these off-site grids were lost, and two diesel generators, one of which was enough to supply the equipment necessary for unit safety.

During reactor operation, core cooling was also ensured through the steam generator feedwater supply, a redundant system. In the event of failure of this system or unavailability of the turbine, the reactor was shut down and water would be supplied to the steam generators by the emergency feedwater system (EFWS), also redundant. The single-failure criterion was thus met.

The first studies on failure of these systems were qualified as ‘beyond-design-basis’ or ‘design boundary’ studies, expressions reserved for studies of serious accidents that were nevertheless of very low probability. These studies examined combinations of failures that had been “left outside the conventional design basis”.

To assess the pertinence and significance of these studies, a basis for evaluation was necessary that would draw on probabilistic references.

13.2. Background of the complementary domain

Based on proposals by the Institute for Protection and Nuclear Safety (IPSN), the notion of combined failures, which was part of what would later be called the ‘complementary domain’, and an initial list of such events were introduced in France by the letter SIN 1076/77 of 11 July 1977 from the Central Service for the Safety of Nuclear Installations (SCSIN)[463]. These aspects were covered again in two ministerial ‘guidance letters’ – CAB 900-MZ of 3 September 1979 and CAB 1121-MZ of

[463] Letter “concerning the major nuclear safety options for units with a pressurized water nuclear reactor that was written by the minister in charge of industry to the chief executive officer of EDF”. This letter, along with letter SIN 576/78 of 16 March 1978 and the two CAB letters mentioned above, are included in the series of texts published by the Directorate for the Safety of Nuclear Installations, 4th edition, issued in May 1999 (published by *Les éditions des Journaux officiels*).

6 October 1983 – concerning the design of 1300 MWe reactors and 1450 MWe reactors, respectively.

The main points of these letters can be summarized as follows:

- facilities featuring a unit that includes a pressurized water reactor must be designed so that the overall probability that this unit may cause unacceptable consequences does not exceed 10^{-6} per year[464];
- the operator is encouraged to use a probabilistic approach for the greatest possible number of events;
- the use of probabilistic approaches does not imply demonstrated compliance with the overall objective described above, nor the direct use of probabilistic methods for unit design, but these approaches may improve the deterministic approach;
- given the overall objective of 10^{-6} for the annual probability of unacceptable consequences, a value of 10^{-7} can be used as an annual probability of unacceptable consequences for an event family, when a probabilistic approach is used for this family;
- it is acceptable, however, to not include event families where the estimated probability is clearly below 10^{-7} per year;
- 'realistic' calculation assumptions and methods may be used to study event families that were chosen according to this extended approach;
- the case of simultaneous failures in redundant systems important to safety must be examined within this framework.

Regarding these principles:

- the overall objective and the objective per event family were set in terms of 'unacceptable consequences', which are not defined by law or regulations. Rather, this is a policy objective that may change over time. In practical terms, each time a probabilistic approach is used for an event family, a cautious and concrete translation of the notion of unacceptable consequences is used, in the form of decoupling criteria[465];
- the probability of 10^{-6} per year of unacceptable consequences is a 'targeted' maximum value. The operator is not asked to demonstrate that this target has been reached. Likewise, the probability of unacceptable consequences of

[464] The probability of 10^{-6} per year and per unit corresponds to a mathematical expectation of 2/1000 that an accident of this type will occur in a nuclear power plant fleet of 50 reactors in operation for 40 years.

[465] For example, for aeroplane crashes, the loss of integrity of a building that houses safety functions is considered to systematically lead to unacceptable consequences. Concerning total failure of redundant systems, initiation of core uncovery due to insufficient cooling water accompanied by the inability to reflood, among other events, is considered as unacceptable.

10^{-7} per year is not an imperative maximum value for an event family, since compensations may exist where other families have lower probabilities;

- the 'complementary measures'[466] that may be revealed as necessary can also include particular operating procedures using systems or components that exist in conventional deterministic design, as well as new systems or components to be implemented, also associated with operating procedures.

This approach has also led to using several event families whose importance has been shown by probabilistic assessments and for which design and operating changes have been considered necessary with, for some of them, the implementation of dedicated operating procedures (referred to as 'H procedures'):

- reactor trip failure during a transient that calls for activating this function. This failure was studied for all Category 2 conditions that involve automatic reactor shutdown. The problematic phenomena that may result are overpressure in the reactor coolant system and under-cooling of the fuel rods. EDF implemented an 'ATWS workaround' to correct such a failure by using different signals, logic systems and devices to trigger a reactor trip;
- total loss of the heat sink or failure of the systems ensuring heat transfer to the heat sink, for which EDF introduced procedure H1;
- total loss of feedwater supply to the steam generators, for which EDF introduced procedure H2, which uses the 'feed and bleed' reactor cooling mode, consisting in cooling the core by water circulation ensured by injection of water in the reactor and voluntary opening of the reactor coolant system via the pressurizer valves[467];
- total loss of on-site and off-site power supplies, for which EDF introduced procedure H3. The analysis conducted by EDF at the time is presented as a reminder in the Focus feature below;
- total loss of the safety injection system or containment spray system, during the long-term phase following a loss-of-coolant accident, for which procedure H4 was introduced. As indicated in Section 17.8, an 'ultimate' procedure, U3, to deal with total loss of water pumping equipment, was added to procedure H4;
- protection of certain riverside sites against flooding above the thousand-year flood level, for which procedure H5 was introduced.

[466] Expression introduced in the letters mentioned above.

[467] Water leaving the pressurizer relief lines is directed to a relief tank equipped with a membrane. When the membrane bursts, the water flows into the reactor building and enters the sumps at the bottom of the containment.

#FOCUS

Analysis of the total loss of on-site and off-site power supplies to a pressurized water reactor[468]

The electrical power necessary for the safety of French nuclear power plants can be supplied in a number of ways (see Figure 13.1):

- two off-site sources from the electricity transmission grid that are relatively independent of each other. One of these sources is called the ‘main power supply line’, which is used for transmission of the electrical energy produced by the reactor. The other line is called the ‘auxiliary line’;
- islanding, during which a plant unit, disconnected from the off-site grids, only operates to supply its own equipment;
- two on-site sources, each consisting of a diesel generator.

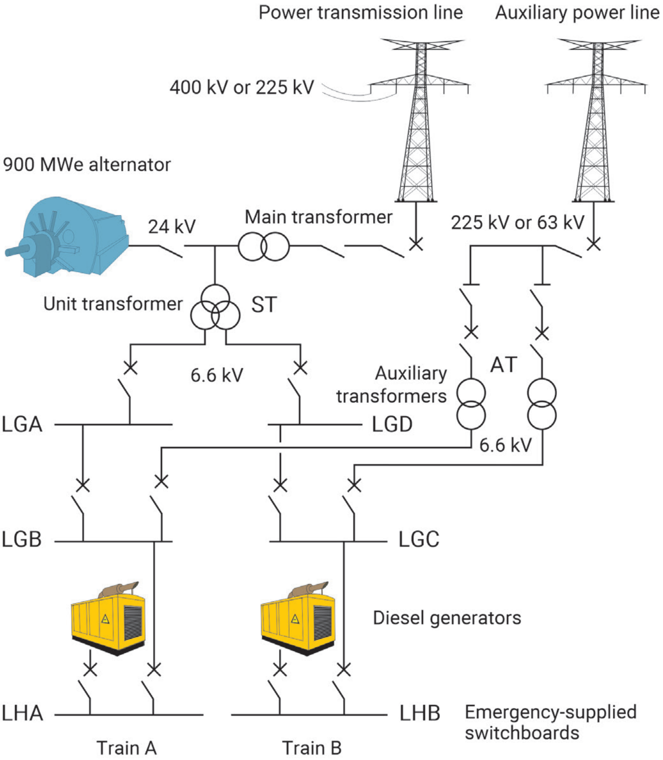


Figure 13.1. Electrical power supply of a 900 MWe reactor. Georges Goué/IRSN.

[468] These developments apply to 900 MWe, 1300 MWe, and 1450 MWe reactors.

Just one of these sources is enough to supply electrical power to equipment necessary to safety. This power supply is distributed via two electrical switchboards, each of which supplies a specific train. Each diesel generator is assigned to one of these two electrical switchboards.

Total loss of on-site and off-site power supplies to equipment necessary to unit safety may result from either the simultaneous failure of all sources, or from that of the two electrical switchboards.

For 900 MWe reactors, in the early 1980s, the probability of total failure of the on-site and off-site power supplies (for one hour) was estimated at 10^{-5} per year and per reactor, with equivalent contributions from source failure and failure of the emergency switchboards LHA and LHB. It was therefore necessary to study the consequences of these failures.

Total loss of on-site and off-site power supplies leads to:

- dropping of shutdown RCCAs and control RCCAs,
- shutdown of all motor-driven pumps,
- immobilization of motor-operated valves, with some of them set to the safe position,
- 'loss' of compressed air, at least after depressurization of the buffer tanks featured in certain systems;
- gradual loss of power in the batteries and, after an hour, 'loss' of all information in the control room and of all possibility of control.

Reactor shutdown by neutron-absorbing rod drop is favourable.

Shutdown of the reactor coolant pumps, equipped with suitable flywheels, is expected in the event of a reactor trip. These flywheels make it possible to switch to natural circulation of the coolant.

Residual heat is removed by the steam generators, supplied with water by the turbine-driven pump(s)[469] of the emergency feedwater system (EFWS) tank. The steam produced is discharged into the atmosphere, since the condenser is unavailable. The EFWS tank features enough capacity to maintain this cooling mode for approximately 20 h.

For 900 MWe reactors, however, it appeared that the hydrodynamic seals on the reactor coolant pumps could be damaged quickly, since shutdown of the chemical and volume control system (CVCS) pumps would interrupted the very-high-pressure water injection to these seals, and shutdown of the component cooling water system (CCWS) would caused loss of the cold water supply to the thermal barrier that helped protect them. They thus showed a high probability of deteriorating, possibly leading to a break in the reactor coolant system. Neither the

[469] Driven by steam from the steam generators.

safety injection system, except for the accumulators, nor the containment spray system could operate in the absence of electrical power. This meant that after a few hours, a particularly serious accident could occur (core uncovery followed by core melting, uncontrolled pressure increase in the containment that could lead to its failure).

EDF thus decided to make certain facility and equipment modifications and introduced operating procedure H3 in order to:

- ensure automatic resupply of water injection to the seals of the reactor coolant pumps, within 2 min, by the reactor coolant system motor-driven test pump[470] (part of the SIS) at a low flow rate, energized by a small turbine generator called LLS. This turbine generator is supplied with steam from a branch connection on the supply line of the EFWS turbine-driven pump. This required mechanical modifications (links between the SIS, CVCS and RCS, and between the LLS and EFWS) and electrical modifications (for the independent start-up and operation of the LLS system, shown in Figure 13.2). This provision was used from the design stage of the 1300 MWe and 1450 MWe reactors, then adapted to equip the 900 MWe units (each 1300 MWe and 1450 MWe reactor has a test pump and an LLS, but there is only one test pump and one LLS for each 900 MWe unit pair);
- maintain minimal instrumentation and control systems in order to: control the water pressure and temperature in the reactor coolant and secondary systems; monitor filling of the reactor coolant system; control the speed of the steam generator EFWS turbine-driven pump(s); and command the atmospheric steam dump valves. The necessary electrical current also comes from the small LLS turbine generator.

In the absence of water letdown of the reactor coolant system, the pressurizer fills up after water injection to the seals on the reactor coolant pumps. The necessary volume is obtained by gradually contracting the coolant fluid by cooling it using the steam generators (at the beginning of the accident at nominal power, the reactor coolant system water, with an average temperature of 286°C, has a density of around 0.7, making it possible to increase volume by around 100 m^3). The first studies showed that it was possible to maintain the fuel in a satisfactory state for about 20 h under these conditions (time period considered sufficient for re-establishing at least one electrical power source, if only temporarily).

Optimization of operating procedure H3 and studying ways to resupply the water tank of the steam generator emergency feedwater system made it possible to extend this period even further.

[470] The test pump is used to pressurize the reactor coolant system during regulatory initial and periodic tests. The supply lines to the reactor coolant pump seals are used for these pressurization operations.

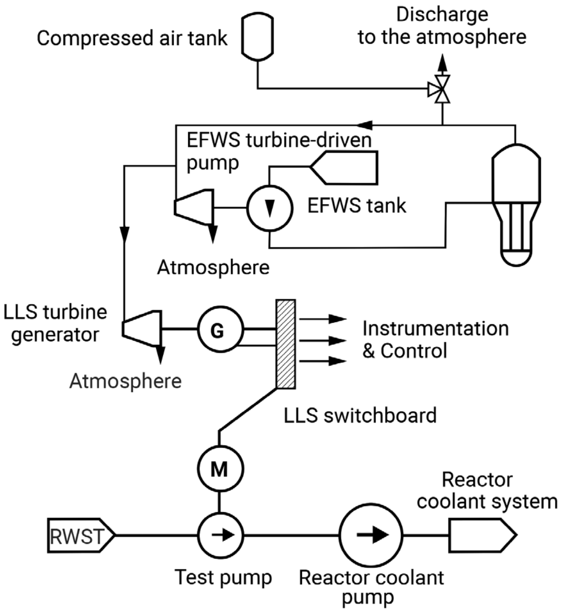


Figure 13.2. Handling the total loss of on-site and off-site power supplies: LLS system. IRSN.

Operating procedure H3 and the associated equipment make it possible to avoid any fuel damage and any significant release of radioactivity.

The time periods were thus sufficient to re-establish electrical power supply in one of the following ways:

- using an off-site source supplied by a unit located either on the plant site, at a neighbouring site, or on a nearby hydraulic unit;
- startup of a mobile gas turbine or a station blackout diesel generator. Either one or the other of these components was added to the possible electrical power sources at each site;
- connection to a generator located on a neighbouring unit, via the connection stand of the gas turbine;
- bypass of the two electrical switchboards assumed to have failed by directly supplying the equipment necessary to safety using the jumper cables that serve for periodic testing.

These provisions were implemented for all the units in service, gradually resolving reliability problems on the relevant systems and components.

13.3. Analysis of complementary domain events

For most complementary domain events (combinations of failures), EDF opted to perform a 'physical' demonstration of the validity of the measures adopted. It was assumed that these studies could be conducted with assumptions having 'less conservative margins' (no aggravating factors, residual heat without a margin or with a reduced margin, response time for the operator set at a value considered reasonable, etc.).

However, implementation of this approach raised a number of questions that pointed to the lack of consistency between the assumptions postulated for the various possible approaches.

Based on this observation, it seemed appropriate to redefine the approach used to inventory the complementary domain events and then study them, with a view to obtaining consistency between the deterministic studies of these events and the support studies used in probabilistic safety assessments.

As part of the process for delivering the operating authorization of Chooz B1 (1996), after the complementary domain events were examined for the N4 series, the nuclear safety authority (DSIN) requested that the operator, EDF, take the following actions:

- re-examine the list of complementary domain events according to a method to be proposed and, if necessary, complete the list, taking into account the results of the probabilistic safety assessments conducted for the N4 series,
- propose an approach for this purpose that states which assumptions have been made and defines 'realistic' methods, so as to exclude any cliff-edge effects, particularly by using sensitivity studies on those parameters that have a strong influence on the relevant transients.

13.4. 'New complementary domain'

These requests by the nuclear safety authority led EDF to propose and apply a new approach for defining the events to be studied, thereby establishing the 'new complementary domain'.

The new complementary domain events are based on the results of the Level 1 probabilistic safety assessments (PSAs) used to verify the conditions of a given safety level. This leads to the possibility of implementing any measures that may be necessary to bring the risk of facility operation to a level considered as acceptable.

In the PSAs, it is possible to take into account systems or components that are not taken into consideration in the deterministic studies of design-basis (reference) operating conditions, and that may have a valuable benefit on safety. These systems and components may play a role in normal operation of the unit (such as the main steam bypass to condenser or to atmosphere [MSBc and MSBa] or water makeup to the reactor coolant system by charging the chemical and volume control system [CVCS]), or they may be specific systems or functions that were not safety-classified at the design stage. The purpose of the (new) complementary domain studies is to verify that all of the provisions implemented actually bring the risk of facility operation to a level considered as acceptable. This verification involves identifying, among the provisions not 'used' in the conventional design-basis demonstration, those that are essential to safety. If necessary, it may involve defining specific additional measures. These physical or operational provisions are called 'complementary measures' and are specific to managing accident situations not covered by the conventional design basis.

In the 'new complementary domain', a 'complementary measure' may be understood as an equipment provision or an operator action that is not preventive (with regard to the initiating event), that is specific to managing accident situations not covered by the conventional design basis and is required in order to ensure that facility safety meets the relevant conditions, considering the probabilistic objectives set.

The main steps required to define the 'new complementary domain' are summarized below:

1. Identification of functional sequences based on the PSA representative of the unit's 'design-basis state', i.e. without taking into account any complementary measures. A 'functional sequence' is defined as a set of probable basic sequences (frequency greater than 10^{-8} per unit and per year) in the PSA model that have common functional characteristics and for which a reduction of the core-melt probability can be obtained by implementing a given complementary measure. This reduction generally depends on a single 'PSA parameter' (such as operator response time or equipment reliability).
2. Each functional sequence used is associated with an event or 'complementary operating condition' that must be studied by the designer to determine a maximum value for the 'PSA parameter', such as the maximum time an operator has to initiate a control action or the reliability of a system or component, considered as a complementary measure.
3. Probabilistic substantiation of the complementary measure: this involves demonstrating that the corresponding probability of core melt is brought to an acceptable level by implementing the complementary measure.

The safety criteria used for deterministic (thermal-hydraulic and physical) studies of events in the (new) complementary domain are the criteria relevant to Category 4 conditions. More restrictive decoupling criteria can be used with regard to the integrity of the various confinement barriers.

The values of physical parameters (quantities characteristic of the unit's initial state, settings for protection thresholds that trigger automatic actions, functional characteristics of systems and components used, residual heat, etc.) are set as follows:

- reasonably bounding values (generally 95%) for dominant parameters,
- nominal values (without uncertainty) for the other parameters.

All systems, components and regulations important to safety (whether 'safety-grade' or not) are taken into account. Systems, components and regulations that are not important to safety can be taken into account on a case-by-case basis, provided their capacity to fulfil their mission is substantiated.

The 'new complementary domain' corresponds to the provisions of the 'INB Order', of which Article 3.2 (Section II) stipulates that, "in addition to the postulated single initiating events, the nuclear safety demonstration covers plausible situations resulting from the combination of initiating events, selected according to criteria substantiated with regard to the analyses and assessments mentioned in Articles 2.7.2 and 3.3."

This approach made it possible to identify or confirm the following complementary measures for 900 MWe units, during their third ten-yearly periodic review:

- automatic isolation of letdown of the chemical and volume control system (CVCS) based on a high temperature criterion;
- isolation of the return water system of the seals on the motor-driven reactor coolant pumps (RCPs) and the CVCS pump miniflow line in case of loss of the component cooling water system;
- manual startup of the 'feed and bleed' cooling mode (see above);
- operation of the LLS turbine generator;
- the water injection system to the seals on the reactor coolant pumps in the event of loss of the 6.6 kV emergency switchboards, the reliability of which was improved during the third ten-yearly outage;
- feedwater supply to the steam generators by the condenser water extraction pumps backing up the turbine-driven auxiliary feedwater pump in the event of loss of the 6.6 kV emergency switchboards;
- gravity-based manual makeup to the reactor coolant system when it is sufficiently open in maintenance outage conditions;
- gravity-based water makeup to the EFWS tank by the demineralized water distribution system;
- water makeup to the reactor coolant system by the CVCS of the neighbouring unit;
- manual 'boration' of the reactor coolant system (this operational measure makes it possible to transfer a boric acid solution at 21,000 ppm of boron);
- the operational measure that aims to provide maximum cooling of the reactor if a reactor coolant system break occurs and high-head safety injection is not available;
- manual startup of safety injection if a reactor coolant system break occurs during normal reactor shutdown with cooling ensured by the steam generators;

- manual startup of safety injection at low pressure if a reactor coolant system break occurs during normal reactor shutdown with cooling ensured by the residual heat removal system (RHRS);
- automatic water makeup to the reactor coolant system if an RHRS loss or break occurs during a maintenance outage;
- manual startup of water makeup to the reactor coolant system if an RHRS loss or break occurs during a maintenance outage and automatic makeup has failed;
- manual switch to water recirculation if an RHRS loss or break occurs during a maintenance outage;
- automatic antidilution protection measures (see Chapter 35);
- mutual backup of the low-head safety injection system (SIS) pumps and the containment spray system (CSS);
- manual water makeup to the pool in the fuel storage building if a pool cooling failure occurs;
- local triggering of the control rod drive mechanism (CRDM) power supply units – these power units allow the gradual RCCA withdrawal or insertion[471];
- station blackout diesel generator;
- 'ATWS workaround';
- automatic shutdown of reactor coolant pumps if the high temperature threshold has been reached on motor bearings and thrust bearings.

The associated equipment items underwent a safety classification and were checked to ensure compliance with operating requirements in the general operating rules.

13.5. Case of the Flamanville 3 EPR

As was the case for the 900 MWe, 1300 MWe, and 1450 MWe reactors, complementary measures were defined for the EPR. They were implemented to handle events that are referred to as RRC-A[472] (Risk Reduction Category-A), i.e. operating conditions with multiple failures.

However, a change of method was introduced by EDF, called for by the provisions of the Technical Directives for the Design and Construction of the Next Generation of Pressurized Water Reactors and the objective of achieving consistency with international practices. The main changes to the approach involve:

[471] Triggering these power units results in loss of electrical power to these mechanisms, which in turn causes the RCCAs to drop by gravity to the point of complete insertion in the core.

[472] In addition, core-melt situations are to be considered in the design phase (RRC-B category). They are covered in Chapter 17.

- the choice of a single reference probabilistic value, set at 10^{-8}, for functional sequences with core melt;
- the design rules for the RCC-A operating conditions with multiple failures: the conditions for considering operator actions are similar to the conditions for deterministic analysis of reference operating conditions (PCCs);
- probabilistic verification of the effectiveness of RRC-A provisions, established through probabilistic safety assessments.

This new ‘renovated’ approach to defining the complementary domain is gradually being implemented for reactors in operation, starting with 900 MWe units, as part of the safety reassessment studies associated with their fourth ten-yearly outage. In this last case, the approach led, first, to confirmation of the provisions already identified in studies on the ‘new complementary domain’, and, second, to using the station blackout diesel generator (SBO DG), a component installed by EDF for extreme situations (operating experience feedback from the accident at the Fukushima Daiichi nuclear power plant – see Section 36.6), as a new additional provision to further reduce risks related to internal reactor events.

Chapter 14
Development and Use of Probabilistic Safety Assessments

This chapter presents the development and use of the Probabilistic Safety Assessments[473] mentioned in chapters 6 and 13 for French nuclear power reactors. The use and importance of these assessments will be illustrated by some of the most significant lessons learned from them, which have led to concrete measures being introduced at plants to enhance their safety.

14.1. History and regulatory context

14.1.1. International situation

▶ The first probabilistic safety assessments

As stated in Chapter 6, the initial design of pressurized water reactors was based on a deterministic defence-in-depth approach.

The first full probabilistic safety assessment (PSA) was developed in the USA in the 1970s and was published in 1975 in the WASH-1400 report, often referred to as the Rasmussen Report (from the name of its principal author, Professor Norman Rasmussen of the Massachusetts Institute of Technology). This assessment, which was not conducted in a regulatory context, aimed to answer the question: does nuclear

[473] Assessments which must be distinguished from approaches of probabilistic nature discussed earlier, for example to take into account certain hazards.

energy pose a risk to the public? The study presented in the WASH-1400 report was a very comprehensive PSA, taking into account a large number of conceivable accident scenarios and making a quantitative assessment of the consequences of these scenarios in terms of the number of deaths as a function of their probability. The results of the study were compared, in terms of probabilities and consequences, to results obtained for other risks of human or natural origin.

Initially the report was widely criticized; its credibility was challenged because of the associated uncertainties. A major turning point came with the Three Mile Island accident in March 1979. After this accident, the Rasmussen Report, which in particular had highlighted the major consequences that could arise from scenarios induced by small breaks in the reactor coolant system of pressurized water reactors, was used more extensively because operators and safety organizations then realized that these PSAs could assess not only the overall risk, but the degree to which different scenarios contribute to that risk and the relative weight of each scenario.

Since then, the development and use of PSAs has continued to grow in terms of the number and types of facilities assessed, the scope of investigations, the various ways PSAs are applied, the importance given to their use, and the research devoted to developing their full potential and reducing uncertainty.

▶ Using probabilistic safety assessments

Specialists from around the world generally agree that the probabilistic and deterministic approaches should be used to complement one another[474] in safety analysis.

The introduction of probabilistic assessments into regulations, however, varies widely from one country to another.

In most countries, PSAs are a regulatory requirement, usually included in periodic safety reviews for existing reactors, but required systematically for new reactor designs. Various guides and standards have been developed on the implementation of PSAs, especially in the USA.

Some countries have even made certain probabilistic targets a regulatory obligation, but to date there is no international consensus on this issue, as questions remain as to how targets and their associated numerical values are to be defined and how compliance with requirements can be demonstrated. Currently, there are three possible situations:

- regulatory probabilistic targets have been set, and demonstrating that they have been met is a requirement, as is the case in the UK;
- targets are published by the regulatory authority and presented as ‘guideline values’ (or other equivalent terms); it is not mandatory to demonstrate that they have been met, but doing so is a factor taken into account in decision-making;

[474] In the sense that probabilistic assessments can provide useful insights to the deterministic approach, which forms the basis of any safety demonstration.

– the regulatory authority does not set any targets, but 'benchmark values' are proposed by operators as a decision-making aid.

▶ Reference levels published by WENRA

The reference levels published by WENRA, the Western European Nuclear Regulators Association, are described in Section 6.6. Some of these reference levels concern the development and use of PSAs.

These reference levels indicate in particular that a Level 1 PSA and a Level 2 PSA must be developed for each nuclear reactor type in service. These PSAs must consider all pertinent accident initiating events, whether of internal or external origin, that are likely to affect the reactor or spent fuel pool. External hazards (earthquake, flooding, extreme temperatures, etc.) must be addressed where the state of the art permits; otherwise, other methods must be used to assess the contribution of external hazards to the risks induced by the facility.

14.1.2. Situation in France

▶ Introduction of probabilistic approaches

As stated in Chapter 13, although the basic design of French nuclear power plants is primarily based on a deterministic approach, when the major technical options envisaged by Électricté de France (EDF) for the 1300 MWe series of reactors were being examined, the Central Service for the Safety of Nuclear facilities (now the French Nuclear Safety Authority, ASN) set out an overall probabilistic target in its letter SIN No 1076/77 of 11 July 1977 in the following terms: "Generally, the design of a unit with a pressurized water reactor should be such that the total probability of that unit causing unacceptable consequences does not exceed 10^{-6} per year. When a probabilistic approach is to be used to assess whether a family of events should be taken into account in the design basis of such a reactor, this family of events must be taken into account if the probability that it would lead to unacceptable consequences is greater than 10^{-7} per year; this value can only be exceeded for the family of events in question if it can be demonstrated that the probability calculations are sufficiently conservative."

Following discussions with EDF, letter SIN No 576/78 of 16 March 1978 clarified the terms of the aforementioned SIN letter. It is worth noting (see Section 13.2) that:

– the overall target is set for 'unacceptable consequences' but these 'unacceptable consequences' are not defined in any legislative or regulatory text; they must be assessed in political terms, taking into account, where appropriate, any site-specific effects and the possibility of population protection measures;

– the probability of 10^{-6} per year is a 'target' value[475] for a unit, but EDF is not required to demonstrate that this target is met.

[475] In practice, the value of 10^{-7} per year and per family of events has been used more often.

▶ The first probabilistic assessments

Probabilistic assessments were then carried out by EDF to assess the probabilities and consequences of the loss of different redundant systems.

Although partial compared with the PSAs that would be developed later on, these early assessments led to the definition of complementary measures, described in Section 14.2.3.

▶ Probabilistic safety assessments covering all internal events

Two probabilistic safety assessments were carried out in the 1980s and published in 1990.

The first PSA for the standardized 900 MWe (CP2) reactors was carried out by IPSN (1983). The second PSA concerning Unit 3 of the Paluel nuclear power plant (representative of P4 type 1300 MWe reactors) was carried out by EDF. Both PSAs aimed to assess core-melt frequency (Level 1 PSA), without taking into account the possibility of internal hazards such as fire, or external hazards such as earthquakes. However, they did consider all operating states, including states where the reactor was shut down, going beyond foreign assessments available at the time.

Both assessments resulted in significant improvements in reactor safety (see Section 14.2.3.).

▶ EPR project

During development of the EPR project, there was a further step forward in the use of probabilistic approaches. The Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, adopted in 2000 by the Advisory Committee for Reactors (GPR) and the German experts involved, explicitly require operators to carry out a Level 1 PSA at the design stage, covering at least the internal hazards, in order to confirm their design choices. The guidelines state that "a significant reduction must be achieved (compared to the units in operation at the time) in the probability of reactor core melt. Implementation of improvements in the defence in depth of facilities should result in a total probability of less than 10^{-5} per year per reactor, taking into account uncertainties, all types of failure and internal and external hazards". These technical guidelines emphasize that, as a general rule, quantitative probabilistic targets should not be considered to be requirements; they are basically intended to serve as guideline values for design verification and assessment.

As will be explained in Section 14.5.1, the probabilistic safety assessments carried out by the designer (Areva), then by the operator (EDF) at the EPR design stage led to significant safety improvements.

▶ Fundamental safety rule

The French safety autority decided to formalize the use of probabilistic approaches in an official text. The text was published in the form of a fundamental safety rule (RFS 2002-01), which describes acceptable methods for performing Level 1 PSAs limited to internal events, and also states how these PSAs may be used.

▶ Introduction of probabilistic assessments into French regulations

From 2008, ASN began to develop a French regulatory corpus, particularly to incorporate the WENRA reference levels.

The Order of 7 February 2012 stipulates that the safety demonstration for basic nuclear installations must be based on a prudent deterministic approach, supplemented by probabilistic assessments of accidents and their consequences. It also requires PSAs to be carried out for nuclear power reactors.

14.2. Level 1 PSA

14.2.1. Scope

The scope of a PSA is defined on the basis of the studied consequences of the initiating events considered and the reactor states chosen for the assessment.

A Level 1 PSA consists of determining all the scenarios (combinations of human error and equipment failures) that can lead to core melt, and assessing their frequency based on the probability of each elementary failure.

The initiating events considered in such a PSA can be placed in two main categories:

- initiating events of internal origin (human error or equipment failures),
- hazards of internal origin (such as fire and flooding) or external origin (earthquake, fire, flooding, tornadoes, etc.).

The initiating events used can also be assessed either for a single facility state (generally the reactor at full power), several states, or all states.

The PSAs developed in France by IRSN and EDF cover all reactor states. As stated earlier, they were the first internationally to include situations that could develop during reactor shutdown states. They cover all initiating events originating inside the facility, loss of off-site power, loss of heat sink, and certain internal and external hazards (see Section 14.4).

The scope of a PSA is not its only important characteristic. Internationally, the care exercised when choosing the methods and data used, particularly the level of detail and quality of the physical and functional studies underpinning the PSA, is quite variable, even though the choices made have a major impact when it comes to using the results to improve facility safety. In France, the data used (such as equipment reliability) for PSAs are representative of the standardized fleet.

14.2.2. Method for carrying out a Level 1 PSA

14.2.2.1. General information

For every initiating event, the accident sequences that can occur due to the success or failure of systems or operator actions involved in ensuring the fundamental safety functions of the reactor are determined in order to assess the frequency of the anticipated subsequent situation (for a Level 1 PSA, this is core melt, as stated earlier). Adding together all the frequency values calculated for the different accident sequences gives the total frequency of the anticipated subsequent situation, making it possible to assess the contributions of the different initiating events and the importance to safety of the corresponding equipment and operator actions. Figure 14.1 summarizes the approach used for Level 1 PSAs.

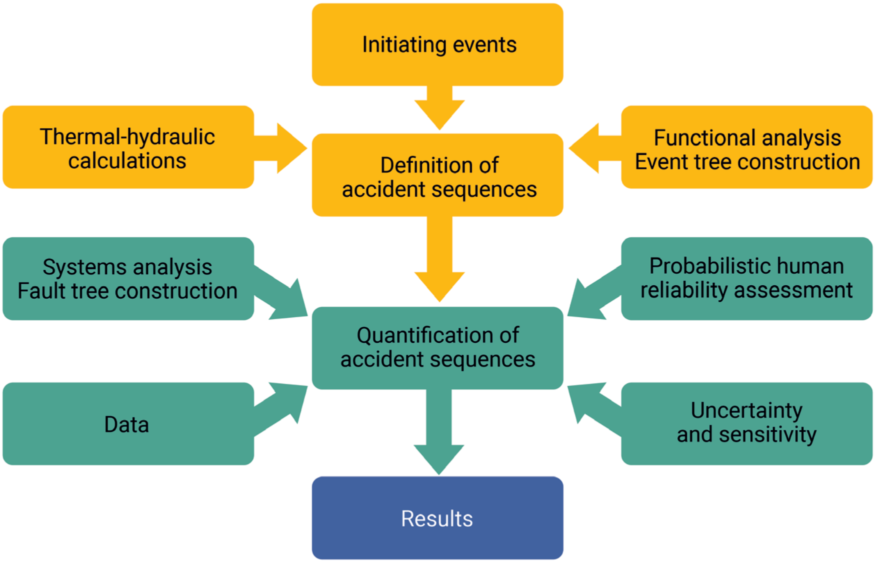

Initiating events
Thermal-hydraulic calculations
Definition of accident sequences
Functional analysis Event tree construction
Systems analysis Fault tree construction
Probabilistic human reliability assessment
Quantification of accident sequences
Data
Uncertainty and sensitivity
Results

Figure 14.1. Approach used for Level 1 PSAs. IRSN.

To begin, there is a qualitative step in which the accident sequences that can lead to core melt are determined from a list of initiating events that is as exhaustive as possible, i.e. events that disrupt the normal operation of the facility and cause certain parameters to drift (pressure, temperature, core reactivity, etc.). This is achieved by constructing an event tree for each initiating event. An event tree is a logic diagram defining the conceivable accident sequences beginning with that initiating event, taking into account the success or failure of the systems or operator actions used to halt progression towards the anticipated subsequent situation. The construction of event trees takes into account any functional dependencies between systems (such as support electrical systems). Each branch of an event tree constitutes an accident sequence for the purposes of the PSA; a thermal-hydraulic study of each branch is carried out to determine whether the sequence could lead to core melt. This study precisely analyses the mission of each system (for example, by determining the number of trains or chains of a system necessary to fulfil the mission) or each operational task (such as the maximum time period allowed to start up a system that may avoid the anticipated situation). Figure 14.2 shows an example of an event tree.

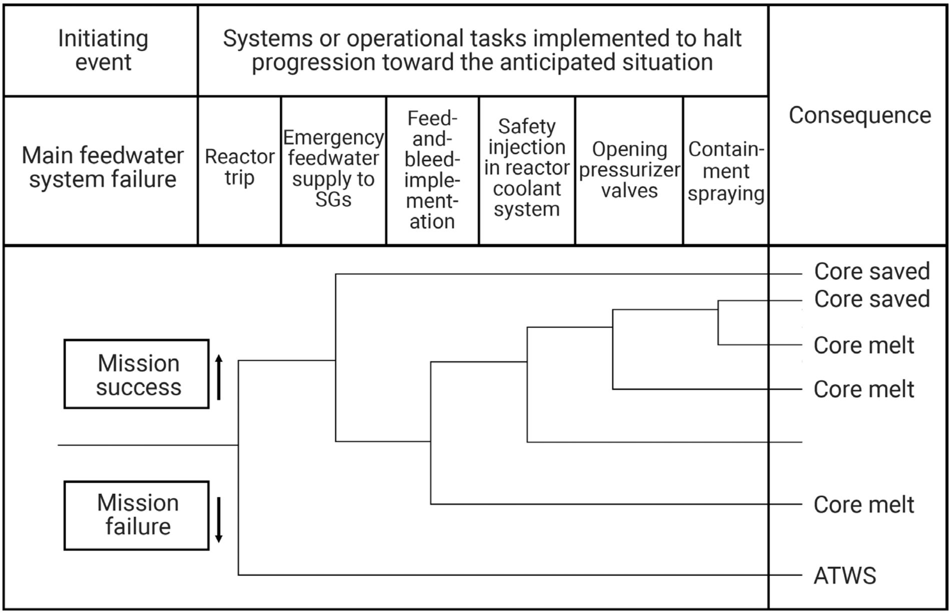

Initiating event
Systems or operational tasks implemented to halt progression toward the anticipated situation
Consequence
Main feedwater system failure
Reactor trip
Emergency feedwater supply to SGs
Feed-and-bleed-implementation
Safety injection in reactor coolant system
Opening pressurizer valves
Containment spraying
Mission success
Mission failure
Core saved
Core saved
Core melt
Core melt
Core melt
ATWS

Figure 14.2. Event tree for the initiating event 'main feedwater system failure with reactor at power'. IRSN.

Once the event tree has been built, there is a quantification stage based on a human reliability assessment and systems analysis. This process identifies failure combinations that can cause missions to fail, and is carried out by constructing fault trees. It quantifies the core-melt frequency associated with each of the accident sequences identified previously. A fault tree is a logic diagram that uses a deductive method to link a system failure to the elementary events likely to cause it. Equipment reliability data for quantifying these elementary events are estimated on the basis of operating experience from EDF reactors.

Figure 14.3 shows an example of system modelling using a fault tree.

When a PSA is intended to cover hazards of external or internal origin, it is not only necessary to have data specific to the hazards being studied, especially the frequency and amplitude of the hazards, but also to determine the initiating events that can occur as a result of these hazards and the specific accident sequences associated with them, along with the systems analysis and human reliability analysis pertinent to the conditions created by these hazards.

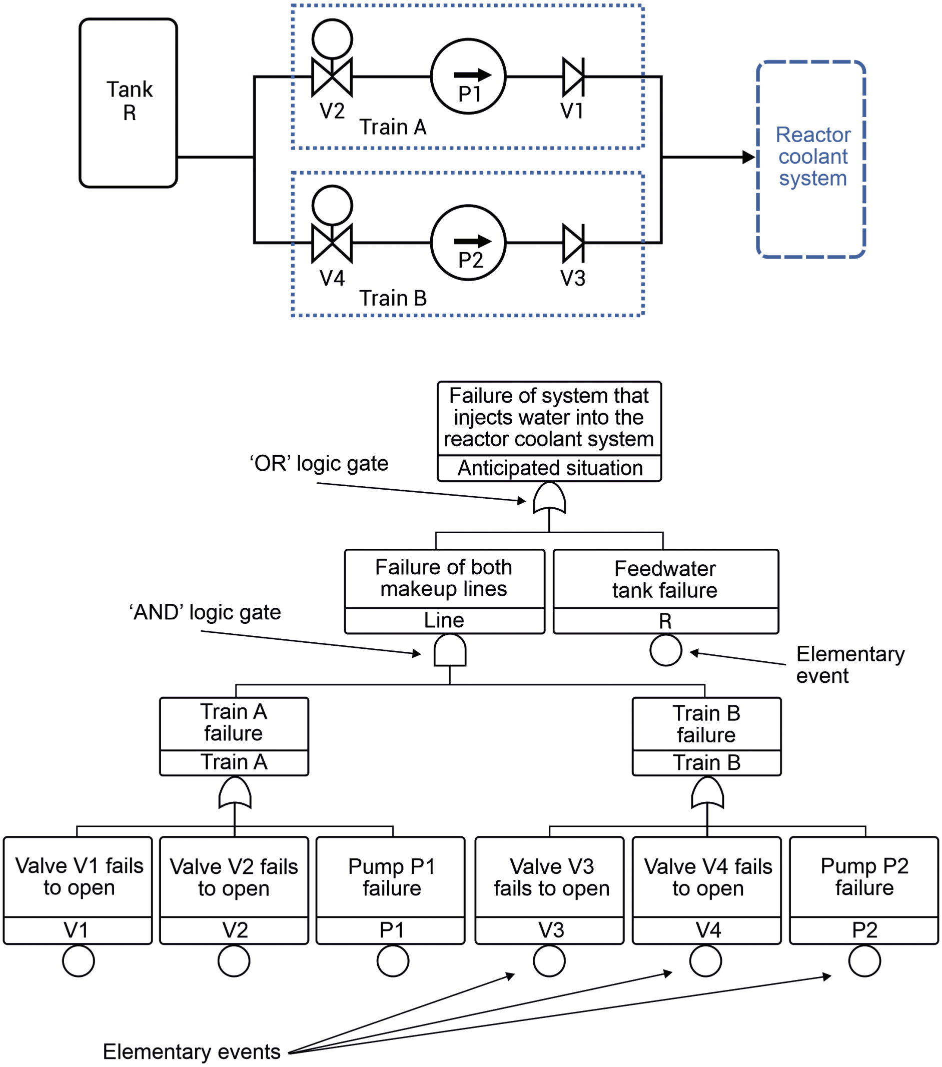


Figure 14.3. Simplified diagram showing a system for water injection into the reactor coolant system (top) and the associated fault tree (bottom). IRSN.

14.2.2.2. Specific point: probabilistic human reliability analysis

An essential part of producing a PSA is the probabilistic human reliability analysis (PHRA), which assesses the probability that operator actions will fail, a difficult task in itself. This can be explained by the fact that it is not easy to systematically collect statistical data on operator actions because, although failures may be counted, the number of actions actually taken is rarely known. A PHRA is therefore based on models that take into account usable data (data on which there is an international consensus, statistics from real-life training of operating crews on simulators, operating experience feedback, etc.) as well as expert opinions.

The first full PHRA model to take into account diagnostic errors, execution errors, inadvertent actions, the context in which the actions are performed, and the dependencies between actions, was the THERP[476] model developed in the USA by Alan Swain. This model is described in NUREG 1278 (entitled Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, August 1983). There are now several dozen PHRA models in existence throughout the world, most of which make partial use of aspects found in previously developed models. The probability tables prepared by Alan Swain are still present in the most widely used PHRA models. However, the most recent models, such as MERMOS, developed by EDF, and ATHEANA, developed by the U.S. NRC, (NUREG 1880 report entitled ATHEANA User's Guide, June 2003, E. Lois), stand out for their use of a functional analysis method that takes into account all the organizational aspects of implementing an operational task, unlike previous methods which were centred on the operator. Some of the disadvantages of this type of method are that it requires costly investment in terms of the time required to perform modelling and validation is more difficult.

▶ PANAME

Since the 2000s, IRSN has used a PHRA model called PANAME for its Level 1 PSAs. PANAME belongs to the family of models containing charts for determining error probabilities based on the time available to perform an operational task, and is largely inspired by the model developed for the first PSAs carried out in France, which in turn was inspired by the US THERP model. It takes into account statistical results obtained by EDF during test campaigns involving operating crews in real-life training on full-scope simulators, i.e. replicas of control rooms at nuclear power plants.

The structure of the PANAME model is based on the organization of an operating crew at an EDF reactor in an incident or accident situation:

- the first module covers the human reliability of the three operators always present in the control room:
    - the Reactor Operator, who is responsible for the reactor coolant system;
    - the Secondary System Operator, who is responsible for the secondary cooling system;
    - the Supervisor, who ensures procedures are correctly followed by the other two operators and thus provides a first level of human redundancy;
- the second module covers the human reliability of a fourth operator who provides support to the crew in the control room during an incident or accident, entering into operation according to the state-oriented approach (SOA, see Chapter 33) and who helps keep the situation in perspective. The fourth operator applies a

[476] Technique for Human Error-Rate Prediction.

specific procedure known as continuous state monitoring (CSM, see Section 33.5) and provides a second level of human redundancy. This role is held initially by the shift manager (SM), and later on by the nuclear safety engineer (NSE).

The first PANAME module makes a distinction between:

– the diagnosis of the situation, which consists of detecting the occurrence of a disturbance requiring the switch to incident or accident operation and correctly following the operating procedures to perform the operational task being assessed probabilistically; the probability of failure ($P_{\textit{Diagnostic failure}}$), a function of the time available, is determined by reading from a graph. The three empirical curves shown in Figure 14.4 form part of the PANAME diagnostic model. They correspond to three scenarios for switching to SOA operation according to different dynamics: in the case of Curve 1, the operators must perform a load reduction; Curve 2 corresponds to the response to an alarm; and Curve 3 corresponds to a reactor trip;

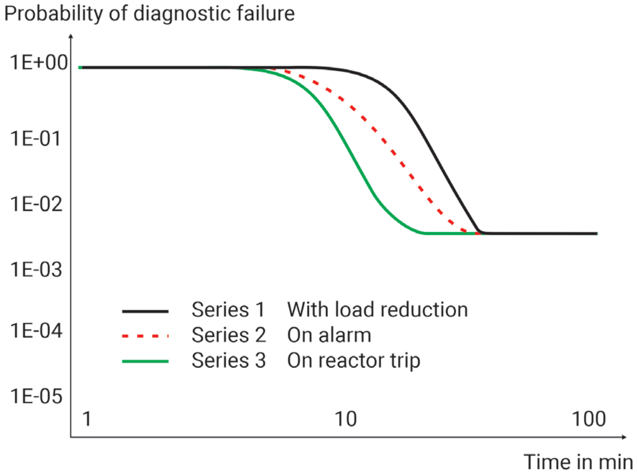


Figure 14.4. PANAME: probability of diagnostic failure as a function of time. IRSN (source EDF).

– execution of the operational task, where the probability of failure ($P_{\textit{Execution failure}}$) is the product of:

- a basic probability of failure ($P_{\textit{Basic failure}}$), the result of statistical processing of real-life training tests with operating crews on simulators carried out by EDF in the 1990s;
- a factor expressing the context (K_f) of the task: 1/3 if the context is ‘easy’ (normal operational task), 1 if the context is ‘normal’ (transient covered in basic operator training), 3 if the context is ‘difficult’ (complex transient), 9 if the context is ‘very difficult’ (coefficient used in particular for hazard situations such as fire);

- a probability of failure of the operating crew to recover from its own errors ($P_{\textit{Non-recovery}}$), a function of redundant requests from the monitoring modules present in the operating procedures, or new requests if the situation deteriorates.

In the output from the first PANAME module, the probability of failure to perform the task before taking into account possible recovery by the fourth operator ($P_{\textit{Failure without SM/NSE}}$) is calculated as follows:

$$P_{\textit{Failure without SM/NSE}} = (P_{\textit{Diagnostic failure}}) + (1 - (P_{\textit{Diagnostic failure}})) \times (P_{\textit{Basic failure}}) \times (P_{\textit{Non-recovery}}) \times (K_f)$$

The probability that the fourth operator (SM or NSE) fails to remedy the error ($P_{\textit{Failure of SM/NSE recovery}}$) is the sum of the probability of the SM and NSE being absent ($P_{\textit{Failure without SM/NSE}}$) as a function of time (EDF statistics) and the probability of their failure when applying the CSM procedure ($P_{\textit{Failure of SM/NSE recovery}}$).

The probability of failure of the operational task $P_{\textit{Task failure}}$ is the product of the probabilities calculated by the two modules:

$$P_{\textit{Task failure}} = P_{\textit{Failure without SM/NSE}} \times P_{\textit{Failure of SM/NSE recovery}}$$

This quick overview shows that time estimates constitute a key element of modelling with PANAME. The model has been enhanced with a tool to calculate the time taken by operators to complete instructions. The tool was based on operating experience feedback relevant to switching to SOA operation as well as expert opinions, and has improved the reproducibility and traceability of results.

▶ MERMOS

The MERMOS[477] model is the most recent PHRA model developed by EDF. It constitutes a departure from the usual format (focused on operator errors, followed by the possibility of recovery by the supervisor, shift manager or nuclear safety engineer), extending instead to the whole operational control system (operating organization, procedures, information available, etc.), while finding malfunctions that will lead to inappropriate control actions. To facilitate modelling, operation is broken down arbitrarily into three functions: strategy, action and diagnostics. For each of these functions, one or more scenarios leading to failure of the operational task are developed. The initial situation is described using a number of ‘Situational Properties’ that generally aim to describe precise elements in terms of operating crew attitude (such as waiting for repair of a component or the late arrival of the fourth operator). The combination of situational properties alone cannot explain a task failure scenario; it is keeping the control system in a particular operating configuration (known as an Important Accident Operation Configuration) for too long that leads to failure. An example showing how an operational task is modelled is presented in Table 14.1 below.

[477] *Méthode d’évaluation de la réalisation des missions opérateurs pour la sûreté* (Method for assessing the performance of operator task for safety).

Table 14.1. Example of how MERMOS models the operational task called ‘Implementation of feed-and-bleed cooling mode’.

	Operational task
	Implementation of feed-and-bleed cooling mode in 60 min after failure of the emergency feedwater supply to the steam generators
	Failure mode
	Strategy error
	Scenario
	The operating crew, hoping to restore operation of the emergency feedwater supply in time, waits too long to implement the feed-and-bleed mode
	Important Accident Operation Configuration
	The control system first attempts to restore operation of the emergency feedwater supply rather than resorting to feed-and-bleed mode because of its consequences
	Situational Properties
SP1	The information sent by the field operators suggests that the emergency feedwater system will be back in operation very soon
SP2	The technical supervisor is heavily involved in actions to restore the emergency feedwater system
SP3	The nuclear safety engineer takes a long time to arrive and does not challenge the operating crew’s strategy

The scenarios modelled using MERMOS, i.e. the probabilities attributed to the Situational Properties and Important Accident Operating Configurations, are quantified on the basis of expert opinions. To make the corresponding studies easier to understand, more robust and more reproducible, the method requires the modeller to select these probabilities from a table of discrete values (see Table 14.2).

Table 14.2. Table of probabilities based on expert opinions used in the MERMOS model.

Expert(s) opinion(s)	Associated probability
Very improbable	0.01
Improbable	0.1
Fairly probable	0.3
Very probable	0.9

Practically speaking, the probability of a failure scenario occurring is the product of the Situational Properties, which describe the initial situation, multiplied by the probability of existence of Important Accident Operating Configurations and by the probability that these continue long enough to cause the task to fail. The total probability of failure of the operational task is obtained by adding together the probabilities of all the scenarios developed for that task, and adding a fixed probability for scenarios that have not been considered by the modeller.

The MERMOS model was developed by a multidisciplinary team of engineers and human science specialists. Its approach aims to take into account the cognitive processes that explain or predict the failure of an operational task. In doing so, it provides information that is useful in designing improvements. Its weaknesses are the quantification of failure scenarios based on expert opinions, and the exhaustiveness of the scenarios it covers.

However, the fact that EDF and IRSN use two very different PHRA models helps to improve the quality of PSAs carried out in France, consequently enhancing safety assessments based on these PSAs.

14.2.3. Level 1 PSA results and lessons learned

It is important to recall that PSAs are tools which must be updated regularly.

EDF has developed Level 1 PSAs for its different reactor models (900 MWe, 1300 MWe and 1450 MWe series) and for the Flamanville 3 EPR, which now serve as a reference base. Updates to this reference base take place at intervals that are directly linked to periodic reviews (performed after commissioning). PSAs are mainly used in the context of these reviews to find ways to improve facility safety.

Working independently, IRSN develops Level 1 PSAs for the 900 MWe and 1300 MWe series, as well as for the EPR. The aim is to provide IRSN with tools to analyse the operator's arguments and to study certain accident scenarios to greater depth. IRSN also uses these PSAs to encourage the operator, during periodic reviews, to propose modifications to facilities and operating procedures in order to improve safety, at the same time taking the opportunity to demonstrate the benefits and feasibility of making certain extensions to the scope of PSAs, inviting the operator to extend the scope of its assessments in consideration of the objectives set for the periodic review. By developing its own PSAs, IRSN is also able to issue pertinent opinions on the probabilistic arguments presented by EDF while units are in operation, for example to assess the acceptability of a request to temporarily waive certain operational limits and conditions.

Although the very first PSAs were limited in scope, they led to the definition and implementation of complementary measures (involving either equipment or operating procedures), such as the small emergency turbine generator (LLS) described in Chapter 13.

Confirming analyses carried out following events in the 1970s and 1980s both inside and outside France, later PSAs, which were broader in scope, led to the introduction of measures aimed at reducing the probability of core melt in shutdown situations where the reactor coolant system was partially drained, i.e. to the level of the reactor coolant loop pipes (mid-loop operation). These events and the measures introduced are described in detail in Section 22.1.

The results presented below are from Level 1 PSAs focused on internal initiating events, developed by EDF and IRSN for the third ten-yearly outage of the 900 MWe reactors (the various assessments carried out as part of the periodic reviews are described in Chapter 30).

EDF's Level 1 probabilistic safety assessment, which took into account modifications made during the third ten-yearly outage, gave a core-melt frequency of approximately 4.6 × 10^{-6} per year per reactor for all scenarios considered.

On completion of its own Level 1 probabilistic safety assessment, IRSN found the core damage frequency[478] to be approximately 7.5 × 10^{-6} per year per reactor, for all reactor operating states. This difference is mainly due to the fact that, for the 'total loss of heat sink' initiating event, the IRSN assessment takes into account depletion of the site water reserves that supply feedwater to the steam generator and uses different probabilistic assessments of human factors. The results of both studies are therefore of a similar order of magnitude. Only the numerical results of the IRSN assessment are shown below (see Table 14.3).

Overall, the results of the assessments by both EDF and IRSN show that the predominant scenarios are those resulting from a loss of off-site power.

Table 14.3. Breakdown by scenario of the calculated core-damage frequency based on Level 1 PSAs conducted by IRSN after the third-ten-yearly-outage for 900 MWe PWRs in the CPY series.

	IRSN assessment (after the update subsequent to the third ten-yearly-outage)	
Scenario type	**Calculated core damage frequency (per year per reactor)**	**% of total core damage frequency**
Loss-of-coolant accidents (LOCA)	1.2 × 10^{-6}	16%
Loss-of-coolant accidents with containment bypass	2.2 × 10^{-7}	2.9%
Secondary system line break accidents	5.0 × 10^{-8}	0.7%
Steam generator tube rupture accidents	1.1 × 10^{-8}	0.1%
Total loss of heat sink or associated systems	1.3 × 10^{-6}	17%
Total loss of feedwater to SGs	1.0 × 10^{-6}	14%
Loss of off-site power	2.9 × 10^{-6}	38%
Loss of on-site power	5.1 × 10^{-7}	6.8%
Transients with reactor trip failure	3.3 × 10^{-8}	0.4%
Transients affecting the reactor coolant system[479]	3.0 × 10^{-7}	4%
Total core damage frequency	7.5 × 10^{-6}	100%

▶ Illustration: sequences induced by loss of off-site power

The following illustration involves accidents that can develop in 900 MWe reactors when a loss of off-site power occurs while the reactor is operating at power.

[478] The expression 'core damage' used here covers situations ranging from those that only lead to cladding failure to those that lead to total in-vessel core melt.

[479] In anticipation, this value incorporates the design and operating improvements prescribed by ASN for non-uniform dilution situations (which are among the transients that can affect the reactor coolant system).

In this situation, a reactor trip occurs and the on-site power supplies (LHP and LHQ emergency diesel generators) are set into operation. If both generators fail, the two 6.6 kV emergency electrical switchboards (LHA and LHB) are no longer powered, leading to a total loss of the emergency power supply system (referred to as an 'H3 situation'). One of the functions of the LHA and LHB electrical switchboards is to supply power to the systems that remove residual heat by means of the emergency feedwater system motor-driven pumps, thereby maintaining the integrity of the reactor coolant system by cooling the thermal barrier of the reactor coolant pumps using the component cooling water system (CCWS) and injecting water in the reactor coolant pump seals using the chemical and volume control system (CVCS).

If the power supply to the 6.6 kV emergency electrical switchboards (LHA and LHB) fails, operator action consists of cooling the reactor using the steam generator auxiliary feedwater pump (AFP-EFWS) and the atmospheric steam dump valves (GCT), in order to reach a fallback state where it is no longer necessary to inject water into the reactor coolant pump seals using the test pump powered by the small emergency turbine generator (LLS) (which avoids a break in the reactor coolant system). This state assumes a reactor coolant system temperature of less than 190°C and a reactor coolant system pressure of less than 45 bars.

In the probabilistic safety assessments, several initiating events that can lead to failure of the LHA and LHB emergency electrical switchboards are considered: the simultaneous failure of the LHA and LHB switchboards (for physical reasons), loss of the main 400 kV line, a short-term loss of off-site power, a long-term loss of off-site power and a grid disturbance.

Figure 14.5 shows the event tree for a long-term loss of off-site power that begins when the reactor is initially generating electricity.

To correctly identify and quantify the accident sequences that can result from this initiating event, it is necessary to take into account accident operation, which requires entering a fallback state as soon as off-site power is lost. Depending on the fallback state of the unit when the subsequent loss of on-site power occurs (emergency diesel generators), the nuclear steam supply system (NSSS) cooling conditions will be different, therefore the resources necessary to manage the situation and the time available to find a power supply source or to 'line up'[480] the station blackout diesel generator (LHT) before core melt will also be different. The assessment uses three time spans for generator failure:

- in the short-term (ST) time span, the onset of an H3 situation occurs quite quickly, i.e. less than two hours after the loss of off-site power. Residual heat is then high and the time to core melt is short, meaning that the LHT diesel generator cannot be lined up if the situation deteriorates; this results in early failure of the feedwater supply to the steam generators or a large-break loss-of-coolant accident due to damage to the reactor coolant pump seals;

[480] Performing all the operations necessary to start up an item of equipment or a system (close electrical switches, open or close valves, etc.).

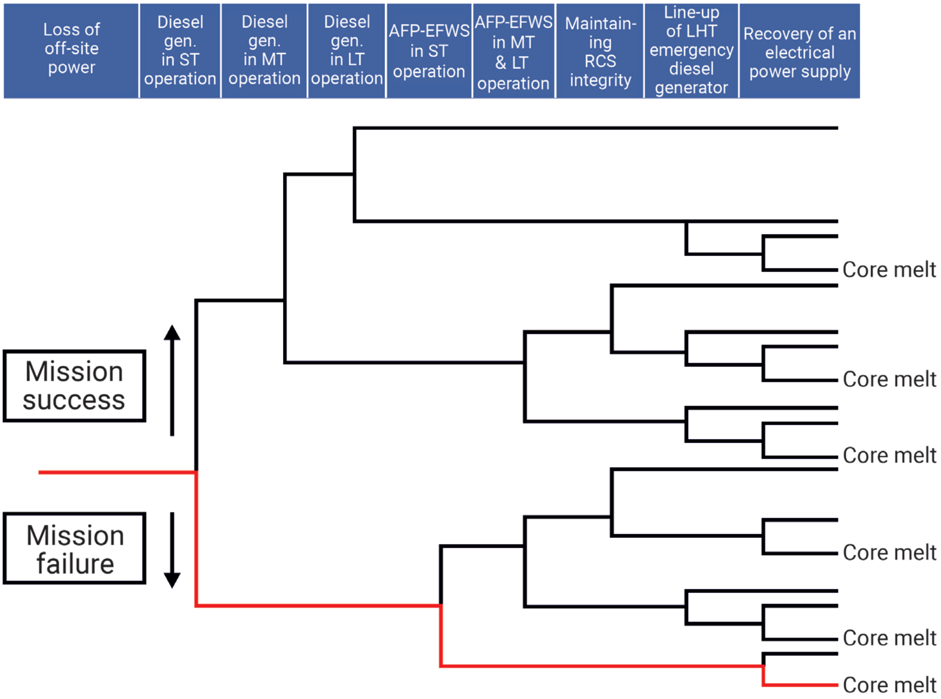

Loss of off-site power
Diesel gen. in ST operation
Diesel gen. in MT operation
Diesel gen. in LT operation
AFP-EFWS in ST operation
AFP-EFWS in MT & LT operation
Maintaining RCS integrity
Line-up of LHT emergency diesel generator
Recovery of an electrical power supply
Mission success
Mission failure
Core melt
Core melt
Core melt
Core melt
Core melt
Core melt

Figure 14.5. Event tree for a long-term loss of off-site power occurring when the reactor is initially generating electricity (ST: short term; MT: medium term; LT: long term). IRSN.

- in the medium-term (MT) time span, the onset of an H3 situation occurs between two and ten hours after the loss of off-site power when the entry into a fallback state is in progress; the time to core melt is longer, allowing the emergency response teams to assemble and providing enough time to line up the LHT generator;
- in the long-term (LT) time span, the onset of an H3 situation occurs more than ten hours after the loss of off-site power; the unit is then assumed to be in the fallback state (reactor under residual heat removal (RHR) conditions, residual heat removal system (RHRS) not connected) when the H3 situation begins. Injection into the reactor coolant pump seals is no longer necessary to avoid a loss-of-coolant accident. The time to core melt is long, allowing the emergency response teams to assemble and providing enough time to line up the LHT diesel generator. This means that if the auxiliary feedwater pump fails, the steam generators can be supplied by a motor-driven pump from the emergency feedwater system.

The accident sequences leading to core melt are thus constructed by considering, for each time span of LHP and LHQ failure, the failure of the means necessary to avoid core melt and loss of a power source during the time available before core melt.

The first sequence in the event tree, starting from the bottom, is the long-term loss of power sources (initiating event) followed by the early failure of both the LHP and LHQ diesel generators and the auxiliary feedwater pump, and failure to recover a power source before core melt; because this happens very quickly, it is not possible to use the station blackout generator (LHT).

To quantify this sequence, it is necessary to know:

- the frequency *F* of the initiating event; this frequency is assessed on the basis of reactor operating experience in EDF's nuclear power plant fleet;
- the probability *P1* of short-term failure of the LHP and LHQ generators; this probability, assessed using a fault tree, takes into account both elementary failures and common-cause failures of the generators, as well as those of the circuit breakers used for the power supply to the emergency electrical switchboards;
- the probability *P2* of short-term failure of the feedwater supply to the steam generators; this probability, assessed using a fault tree, takes into account both elementary failures and common-cause failures of all components involved in this task, particularly the auxiliary feedwater pump, emergency feedwater system valves, etc.;
- the probability *P3* of non-recovery of a power source (off-site power or LHP or LHQ diesel generator) before core melt (the time to core melt in this situation is approximately one hour).

Based on this data, and provided that the different events considered are independent, the probability of the accident sequence in question is the product of $F \times P1 \times P2 \times P3$.

14.3. Level 2 PSA

14.3.1. Scope

Level 2 probabilistic safety assessments aim to extend the core-melt accident sequences identified by the Level 1 PSAs by determining the progression of these accidents and the associated radioactive releases in terms of frequency, amplitude and kinetics. Like the Level 1 PSAs, Level 2 PSAs were first developed to study the risks associated with internal accident initiating events (reactor at power or shut down).

EDF and IRSN first produced Level 2 PSAs for the 900 MWe reactors and, later, for the 1300 MWe reactors. A Level 2 PSA was also produced by EDF for the Flamanville 3 EPR, which includes accident sequences that lead to fuel cladding failure (without fuel melting) and can be used to assess the scope of these situations.

As with Level 1 PSAs, the reference assessments are those conducted by EDF, with IRSN developing assessments independently so that it can carry out analyses pertinent to the arguments presented by the operator.

14.3.2. Method for carrying out a Level 2 PSA

14.3.2.1. General information

An accident scenario in the Level 1 PSA leading to fuel damage and therefore the possibility of fission product release into the environment can in fact lead to variable release levels depending on:

- whether or not certain physical phenomena arise (particularly hydrogen combustion or a steam explosion),
- the equipment failures induced, for example, by an energy-related phenomenon (such as combustion) or by the ambient conditions caused by the accident,
- operator actions and any associated human errors,
- restarting of equipment during the accident.

In practice, a Level 2 PSA is built on the basis of:

- an interface with a Level 1 PSA,
- a 'severe accidents' event tree, used to combine all events and phenomena likely to occur and then establish accident development scenarios leading to different types of consequences,
- a system of presenting results based on categories of release.

Many physical support studies must be carried out.

Figure 14.6 shows a schematic diagram of the method generally used to produce a Level 2 PSA. Radiological impact assessments can be used to assess the severity of accident situations.

▶ Interface with the Level 1 PSA

Creating an interface with a Level 1 PSA is the first step in carrying out a Level 2 PSA. This interface must:

- ensure that relevant information on the damaged reactor state at the time of core melt (particularly the state of engineered safety systems, the confinement state, the reactor coolant system pressure, etc.) is incorporated into the Level 2 PSA, i.e. information that could have a significant influence on the subsequent progression of the accident, particularly the possible failure modes of the containment and the extent of any release;
- create groups of sequences, from the thousands of Level 1 PSA accident sequences, that lead to a similar subsequent development; these groups of sequences define the plant damage states (PDS).

Depending on the assessment methods used and the desired level of detail required for applications, several dozen to several hundred plant damage states may be identified when conducting a Level 2 PSA.

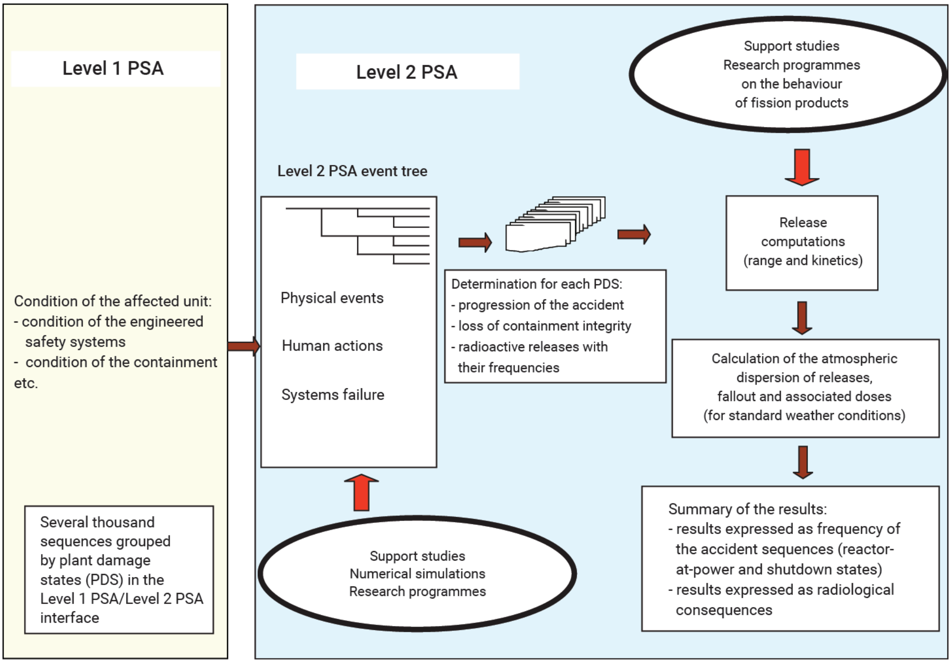

Level 1 PSA
Condition of the affected unit:
- condition of the engineered safety systems
- condition of the containment
etc.
Several thousand sequences grouped by plant damage states (PDS) in the Level 1 PSA/Level 2 PSA interface
Level 2 PSA
Level 2 PSA event tree
Physical events
Human actions
Systems failure
Support studies
Numerical simulations
Research programmes
Determination for each PDS:
- progression of the accident
- loss of containment integrity
- radioactive releases with their frequencies
Support studies
Research programmes on the behaviour of fission products
Release computations (range and kinetics)
Calculation of the atmospheric dispersion of releases, fallout and associated doses (for standard weather conditions)
Summary of the results:
- results expressed as frequency of the accident sequences (reactor-at-power and shutdown states)
- results expressed as radiological consequences

Figure 14.6. Method for carrying out a Level 2 PSA. IRSN.

▶ Severe accident event tree

The main focus of the Level 2 PSA is an event tree that describes all the events that could affect the development of the accident, from fuel damage to the release of radioactive substances into the environment. The plant damage states are the initiating events of this event tree.

The 'nodes' of this event tree represent models of the conditional probabilities of occurrence and the consequences of:

- physical events (for example, core damage and the formation of a corium pool, cladding oxidation and hydrogen production, induced breaks[481] in the reactor coolant system, steam explosions inside or outside the reactor vessel, direct heating of gases in the containment if the reactor vessel fails under pressure, concrete basemat erosion by corium, combustion of flammable gases);
- human actions recommended in the 'Severe Accident Operating Guidelines' (see Chapter 17); for example, depressurization of the RCS, containment isolation, water injection (under certain conditions) to cool the reactor core or corium in the vessel, cooling by the steam generators, startup of the containment spray system, startup of the containment filtered venting system);

[481] Breaks caused by an excessive increase in reactor coolant system pressure and temperature.

- errors made when applying the guidelines;
- failure of structures, systems or components (for example, mechanical failure of the containment as a result of a pressure increase or excessive temperature, loss of leaktightness at penetrations, etc.).

The event tree is used to determine the possible developments of each accident scenario identified by the Level 1 PSA, the associated consequences (containment failure, nature and extent of release into the environment) and their annual frequency of occurrence.

Different approaches can be used to construct such an event tree:

- simplified approaches, which aim mainly to assess the frequency of any significant release;
- detailed approaches: in this case, the event trees include more detailed modelling of each physical phenomenon, human action or system configuration, and rely on variables that describe the reactor state fairly precisely at each stage of accident development.

The Level 2 PSAs carried out by EDF take the first approach and have gradually been extended. For operational reasons, EDF wanted to limit the complexity of its Level 2 PSAs.

Assessments conducted by IRSN take the second approach. In particular, the decision was made to prioritize the use of simulation by computer codes rather than the use of expert opinions to develop models for the ‘severe accident’ event tree. This led IRSN to develop special methods (KANT software for developing and quantifying event trees, release calculation model, etc.) to improve its simulation tools (ASTEC in particular, which can be used for a complete simulation of a reactor in a core-melt accident situation – see Chapter 40) and for conducting particularly detailed studies.

The assessments carried out by IRSN and those conducted by EDF are technically independent of each other, allowing IRSN to examine EDF’s assessments with greater insight.

Generally, quantification associated with physical events takes into account the current state of knowledge and, if necessary, is updated. However, for some subjects (hydrogen explosions, deflagration-detonation transition, energy interaction between corium and water, ultimate strength of containment or certain components), the models used show a high degree of uncertainty. In this case it is useful to carry out sensitivity studies or uncertainty assessments.

▶ Release categories

Radioactive release cannot be assessed for every accident sequence of a Level 2 PSA. Consequently, sequences are grouped into a limited number of release categories, each one associated with a containment failure mode, as well as the amplitude and kinetics of each type of radioactive release. The failure mode, amplitude and kinetics of these release groups can then be estimated using core-melt-accident computer codes, such as ASTEC or MAAP (see Chapter 40), or simplified models developed specifically for Level 2 PSAs.

The frequency and characteristics of the types of release associated with the different release categories constitute the final result of a Level 2 PSA.

▶ Support studies for Level 2 PSAs

Developing a Level 2 PSA requires conducting a large number of support studies to realistically describe the different Level 2 PSA sequences and quantify the frequency associated with each one.

Table 14.4 presents a list of the aspects to be studied in the case of a pressurized water reactor.

Established for the FP7-Euratom ASAMPSA2 project[482], this list illustrates the fact that defining and carrying out support studies, in practice, makes up most of the work involved in conducting Level 2 PSAs. These support studies are largely based on research findings on core-melt accidents.

Table 14.4. Studies required in order to produce a Level 2 PSA for a pressurized water reactor.

Level 1 PSA/Level 2 PSA interface
Level 1 PSA sequences that lead to the same type of core-melt accident progression, particularly in terms of containment failure mode and extent of release, are grouped together in plant damage states. Scenarios leading to core melt are investigated. For accidents induced by a hazard (such as earthquake or flooding) – see Section 14.4 – the interface can include the impact of the hazard on the structures, systems and components useful for subsequent management of the core-melt accident (such as the containment)

Probabilistic human reliability analysis (PHRA)
Identification of the human actions that may occur during a sequence (actions set out in the Severe Accident Operating Guidelines, emergency response support media, equipment repair, etc.)
Quantification of the probabilities of failure of the various operator actions required in the event of a core-melt accident

[482] The purpose of the ASAMPSA2 project was to develop best practice guidelines for the development and implementation of Level 2 PSAs based on feedback from 21 European partners involved in reactor safety. The project ended in 2012.

Quantification of the physical phenomena and resulting loads for the containment ***In-vessel accident progression phase***
Study of the progression of each accident up to 'severe accident' onset (thermal-hydraulics of system lines, activation and configuration of engineered safety systems, time available, operator actions, etc.)
Fuel degradation
Rupture of the reactor coolant system including rupture of the steam generator tubes induced by a high-pressure core-melt accident
Hydrogen production
Recovery of core cooling (injection of water in the reactor coolant system)
Vessel cooling from outside through flooding of the reactor pit
Investigation of the consequences of in-vessel water injection (corium cooling, increase in the kinetics of hydrogen production by oxidation of zirconium in the cladding, rise in vessel pressure, etc.)
Investigation of the composition of the containment atmosphere (role of hydrogen recombiners, role of containment spray system) and any possible rise in the containment pressure
Effects of opening the containment filtered venting system
Studies on the distribution and combustion of hydrogen released into the containment
Investigation of the risk of criticality from corium
Investigation of the possibilities of in-vessel steam explosion and the associated consequences (leaks in the reactor coolant system, mechanical failure of the vessel, loss of containment integrity)
Investigation of the conditions of a vessel rupture (time before rupture, type of rupture, etc.)

Quantification of the physical phenomena and resulting loads for the containment ***Vessel rupture phase***
Investigation of the phenomenon of direct containment heating if the vessel breaks while it is pressurized
Investigation of the consequences of a steam explosion in the reactor pit
Investigation of the risk of criticality from corium

Quantification of the physical phenomena and resulting loads for the containment ***Phase following vessel rupture, with corium in the reactor pit***
Corium coolability conditions
Radial and axial erosion of the reactor pit walls and basemat (molten core-concrete interaction)
Impact of water injection into the reactor pit (corium cooling, rise in containment pressure)
Assessment of the production of non-condensable gases (H_2, CO, CO_2, etc.) and steam during the molten core-concrete interaction
Investigation of the change in the composition and pressure of the containment atmosphere

Investigation of the distribution and combustion of hydrogen and carbon monoxide released into the containment
Effects of opening the containment filtered venting system

Investigation of containment performance (integrity)
Investigation of the containment leakage rate before the accident (normal leakage rate, possible losses of integrity on certain devices between two periodic tests)
Investigation of the reliability of the containment isolation system
Assessment of containment performance (integrity) under core-melt accident conditions: 1. Mechanical response of the containment when subjected to quasi-static or slow pressure or temperature loads. Assessment of the maximum mechanical strength and fragility curves of the containment. Assessment of the size of any resulting break 2. Assessment of the response of the containment assumed to be subjected to specific loads (effects of a steam explosion in the reactor pit on the adjacent structures, effects of a local hydrogen deflagration, etc.)
Assessment of containment penetration performance (integrity) under core-melt accident conditions
Identification of possible containment bypasses (such as pipes in the basemats of certain containments)
Investigation of confinement functions in auxiliary buildings (ventilation, filtration, dynamic confinement, etc.)

Investigation of equipment behaviour under core-melt accident conditions
Recirculation and cooling of condensed water in the containment (removal of heat from the containment)
RCS safety valves (reliability of RCS depressurization under core-melt accident conditions)
Steam generators (integrity of the steam generator tubes, steam generator cooling efficiency)
Instrumentation (availability of reactor instrumentation under core-melt accident conditions)
Passive systems (hydrogen recombiners, etc.)
Core catcher for the EPR

Quantification of radioactive release outside the containment
Identification of key parameters for assessment of radioactive release and definition of release categories
Categorization of fission product (FP) isotopes according to volatility class (volatile FPs, noble gases, semi-volatile or low-volatile FPs) and their physical form (aerosol or gas) in the containment
Calculation of release for representative sequences using codes such as ASTEC, MAAP or MELCOR, or simplified models developed specifically for Level 2 PSAs

14.3.2.2. Probabilistic human reliability analysis for Level 2 PSAs

The decision to take actions recommended in the Severe Accident Operating Guidelines would be made in a context where an emergency response organization has been implemented.

To model the human reliability of this organization, IRSN has developed a specific probabilistic human reliability assessment (PHRA) model known as HORAAM[483].

The HORAAM model is based on the decision tree technique, which represents the possible consequences of a fairly complex situation as a tree, with the consequences of decisions made shown at the branch tips. In the HORAAM model, the decision tree summarizes all the conceivable human intervention situations in a core-melt accident, using seven parameters as the influencing factors (time required, difficulty, and others; see Table 14.5). Each of the parameters has two or three possible values (short/medium/long, easy/difficult, etc.). Each branch of the tree represents a type of human intervention and is assigned a probability of failure.

Human interventions carried out at the request of the emergency response organization are part of the 'information-decision-action' process. The information phase is extremely important because the emergency response teams need information that is as clear as possible as quickly as possible to assess the situation.

The decision phase is the primary cognitive phase: the emergency response teams try to understand what is happening, to determine the state of the facility and how it is likely to evolve, to assess the present and future consequences and, based on these factors, to reach a decision and deliver it to others, within a time window limited by the accident kinetics. This phase involves making choices despite uncertainty and the need to make compromises between potentially contradictory objectives. The parameters with the greatest influence on the success of this phase are the time taken to make the decision, the difficulty of understanding the unfolding accident scenario, and the difficulty of reaching a decision.

The action phase takes place at a local level. The parameters with the greatest influence on the success of this phase are the difficulty of the actions to be performed by the operators (task complexity) and the difficulties caused by the physical conditions of task performance (degree of danger, strenuous conditions, etc.).

The seven influencing factors that form the structure of the HORAAM model were chosen on the basis of operating experience from emergency response exercises. These exercises (see Chapter 38), carried out regularly in France to train the emergency response organization, consist of performing staged accident scenarios using EDF's operational simulators.

Table 14.5. Definition of influencing factors in the HORAAM model.

Influencing factor	Description
Measuring systems and means of information	Quality and reliability of all measurements taken and of information provided in the control room and the means of delivering this information to the emergency response teams (fax, telephone, automatic data transmission from the damaged reactor, etc.)

[483] Human and Organizational Reliability Analysis in Accident Management.

Influencing factor	Description
Decision-making time	Time required to obtain information, check it, process it and make a decision on action to be taken
Decision-making difficulty	Difficulty of taking a decision
Difficulty of the scenario	Difficulty related to the overall decision-making context, such as the type of accident or the rate of change in the transient situation
Degree of involvement of emergency response teams	Number of operating crews or emergency response teams involved in the decision-making process: operating crew only, local emergency response team on site or national emergency response organization
Difficulties caused by physical conditions	Difficulties related to the conditions in which the action decided upon must be performed (for example, radioactive environment, lighting, temperature, presence of smoke or gas, lack of space)
Difficulty for operators	Difficulty of action decided upon, regardless of the conditions of intervention: quality of procedures, operator experience in the operational task to be performed

Quantification in the HORAAM model (i.e. assignment of probabilities to the different branches of the decision tree) is complex, especially due to the fact that the influencing factors in the model are not independent of one another. For quantification, IRSN carried out a vast campaign of interviews with emergency response team members within both IRSN and EDF. As a result, it formalized a method that could incorporate these experts' responses by observing which trios of factors had the greatest influence on the success or failure of an operational task. On the whole, the HORAAM model is based on expert opinions with regard to validation of the influencing factors, their ranking in order of importance and quantification of the decision trees.

The HORAAM model was developed on the basis of observations from staged emergencies, but also took into consideration lessons learned from the accident in March 2011 at the Fukushima Daiichi nuclear power plant. Comparison with a real-life situation showed that the influencing factors chosen for the model were generally pertinent.

For its Level 2 PSAs, EDF developed the generic PHRA model known as MEPEM[484]. This model is based on methodological contributions from the MERMOS model, with forecasting added to the diagnostics, strategy and action functions of the MERMOS model. The forecasting function takes into account the emergency response teams' collective assessment of how the situation may evolve. However, in the absence of the data required to develop operational task failure scenarios, particularly in the case of sequences grouped within the same plant damage state leading to several different operating configurations, MEPEM can be used to produce lump-sum assessments by providing bounding probabilities. In this manner, the diagnosis, strategy, forecasting

[484] *Méthode d'évaluation probabiliste de l'échec des missions facteurs humains* (Method for a probabilistic assessment of mission failure, based on human factors).

and action functions can each be assigned a probability of failure from a scale of discrete values (1×10^{-3} for almost impossible failure of the function, 1×10^{-1} for unlikely failure of the function, etc.).

In both its qualitative and quantitative phases, modelling of an operational task in a core-melt accident situation using the MEPEM method is based on expert opinions.

14.3.3. Examples of lessons learned from Level 2 PSAs

The results of a Level 2 PSA can be used to identify the main sequences contributing to the risk of radioactive release, as well as those sequences for which equipment changes or modifications in human action could significantly reduce this risk. In addition, through the support studies carried out for these PSAs, new knowledge is acquired on facility behaviour. Some examples of lessons learned from Level 2 PSAs for reactors (prior to the Flamanville 3 EPR) are presented below.

14.3.3.1. Steam explosion risk assessment

The results of IRSN's Level 2 PSA and the support studies carried out for the 900 MWe reactors led to clarification of the risks associated with a steam explosion in the reactor pit.

These reactors feature a passageway between the reactor pit and the upper part of the containment. Operation of the containment spray system therefore leads to the presence of water in the reactor pit. If core melt and vessel melt-through occur, corium at a temperature of approximately 1700°C could flow into the water in the reactor pit, potentially causing an explosive phenomenon known as a steam explosion.

According to the results of certain calculations, the explosion could generate vibrations violent enough to compromise the integrity of the containment. However, significant uncertainty exists regarding the results of these calculations.

The advantages and disadvantages of different possible strategies for corium cooling outside the vessel have been the subject of much debate between EDF and IRSN (although the presence of water in the reactor pit before corium melt could lead to a steam explosion, the presence of this water also slows down the molten corium-concrete interaction), especially during periodic reviews of the different plant series, requiring additional studies and research. However, in the framework of the third ten-yearly outage of the 1300 MWe units, IRSN considered that measures should be prioritized to ensure the reactor pit was dry at the beginning of the accident and to stabilize any corium in the event of reactor vessel failure. The feasibility of these measures, which are similar to those used for the Flamanville 3 EPR – where measures were taken at the design stage by installing a special core catcher – was examined by EDF in the context of the fourth ten-yearly outage of the 900 MWe units. The option chosen by EDF was to allow corium to spread in the dry reactor pit and an adjacent room, followed by reflooding (see Section 17.5.7).

14.3.3.2. Mechanical integrity of the 900 MWe reactor containments

The 900 MWe reactor containments were designed to ensure their mechanical integrity and leaktightness against an absolute internal pressure of approximately 5 bars in loss-of-coolant accident conditions. Each containment has an internal steel liner to ensure it remains leaktight. The mechanical strength and integrity of containments are checked periodically, particularly during ten-yearly air pressure tests at 5 bars absolute pressure. Considering the vital role the containment can play in mitigating the risk of core-melt accidents, it seemed appropriate to try to assess the ultimate mechanical strength of containments beyond their design pressure. As a result, mechanical strength tests were performed on containment mock-ups, and detailed models were developed to assess the mechanical behaviour of these containments using numerical simulation.

IRSN thus carried out detailed mechanical studies of containments, modelling specific areas using a fine mesh, particularly in the equipment hatch area. The mesh is shown in Figure 40.5 of Chapter 40, devoted to simulation software.

Based on the results of the mechanical strength tests performed using mock-ups and the results of numerical simulation, IRSN and EDF found that the containment walls retained a satisfactory level of mechanical strength and leaktightness up to well above their design pressure (to about 10 bars absolute pressure), but that the equipment hatch closure system was a relative weak spot in terms of pressure resistance.

Certain studies conducted by IRSN to support its Level 2 PSA for the 900 MWe PWRs have shown that, for certain phenomena that may occur during a core-melt accident (direct containment heating caused by mechanical failure of the vessel under pressure, hydrogen combustion after in-vessel core reflooding), the loads calculated could affect the leaktightness of the equipment hatch closure system, leading to radioactive release into the environment.

EDF therefore decided to reinforce the equipment hatch closure system on 900 MWe units, during their third ten-yearly outage. The designed reinforcement ensures the integrity of the equipment hatch up to a pressure of 8 bars absolute pressure, which is significantly higher than the design pressure of the containments.

For IRSN, the gains achieved by reinforcing the equipment hatch closure system are considerable: a reduction of a few 10^{-7} per year per reactor in the estimated frequency of accidents leading to loss of containment integrity in the event of direct containment heating or hydrogen combustion.

14.3.3.3. Isolating penetrations in the containment

A Level 2 PSA entails a detailed examination of the possibilities of failure on containment isolation valves. The studies conducted by IRSN to support the Level 2 PSA for the 900 MWe reactors revealed risks associated with failure of the manual isolation of certain containment penetrations in the event of total loss of power supplies. This was confirmed by EDF during the development of its Level 2 PSAs, prompting it to define special measures for closing the penetrations in question (priority to be given to local closing action on motorized containment isolation valves, installation of electrical backup systems for the relevant valves, etc.).

Level 2 PSAs also established the importance of taking measures (in terms of equipment and procedures) to reclose the equipment hatch during core-melt accidents, including situations where there is a total loss of power supplies.

14.3.3.4. Modifying the pressure relief system of the reactor coolant system

A depressurized vessel is essential in the event of core melt in order to mitigate the risk of radioactive release.

The Level 2 PSAs carried out by EDF and IRSN led to the examination of two possibilities for improving the reactor coolant system's protection and relief valves installed in 900 MWe, 1300 MWe and 1450 MWe reactors:

1. Each valve is driven by an electrically powered 'control pilot' that receives the command to open the valve. In the original design, cutting off the power supply to the control pilot would cause the valves to close. This meant that there was a risk of valve closure during the in-vessel core-melt phase, covered by the Level 2 PSAs.

2. Because of their initial mechanical design, the valves in question reclose at a pressure of about 9 bars if the containment pressure is at atmospheric pressure. This reclosure pressure increases as the containment pressure increases, up to 18 bars for a containment pressure of 5 bars.

Further measures were defined by EDF to ensure adequate depressurization of the reactor coolant system in a core-melt accident situation, consisting of the following:

- the possibility of providing a backup power supply to the valves from portable batteries and modifying the control pilot design to ensure the valves stay open after the open command, even if the power supply to the control pilot fails;
- modification of the valve head design to significantly reduce the valve reclosure pressure and eliminate interdependence with containment pressure; this modification provides better control of the reactor coolant system pressure in an accident situation, limits the effects associated with vessel failure under pressure in a core-melt situation, and facilitates the use of an ultimate low-pressure injection of water, if necessary.

14.3.3.5. Improvement of operating procedures to reduce risk of core melt under pressure

When the periodic review associated with the third ten-yearly outage of the 1300 MWe reactors was carried out, in coherence with the results of its Level 2 PSA, EDF made changes to its operating procedures in order to improve reliability when reactor coolant system depressurization is performed by operators. This action is essential to preserving containment integrity (discussed further in Section 17.10.3).

14.3.3.6. Contribution of Level 2 PSAs to emergency response measures

Level 2 PSAs and the associated support studies have generated a vast amount of knowledge that can prove useful for emergency response. For example, work conducted by IRSN has led to:

– consolidation of the resources devoted to IRSN's emergency response centre (by writing summary information sheets on the possible ways a core-melt accident could develop for each reactor type, by improving computerized tools for assessing predictions of release into the environment, etc.),

– contributions to the documents prepared on the post-accident phase of a core-melt accident in a pressurized water reactor, for example by providing representative scenarios for these accidents.

Studies carried out to support IRSN's Level 2 PSA also highlighted the advantage for operators and emergency response teams of having a means of detecting vessel failure in a core-melt accident[485]. If the RCS remains pressurized without any influx of water, vessel failure will inevitably occur shortly after corium reaches the vessel lower head. In other cases, however, major uncertainties exist as to the time from corium melt to vessel failure (and even whether failure will occur). Yet it is essential for the long-term management of a core-melt accident to know whether or not corium has breached the vessel.

This topic was examined during the third periodic review of the 900 MWe units; since then, EDF has installed a vessel breach detection device in all units.

14.4. Expanding the scope of PSA coverage

The issue of whether the scope of PSAs conducted by operators should be extended (to cover more than just events of internal origin) has led to long discussions in France.

The first step forward was taken in 2007, when ASN asked EDF to take into account certain hazards in Level 1 PSAs, such as earthquake, internal explosions and flooding, so that the benefits of modifications, in terms of safety, could be assessed by considering the most plausible hazards.

The Fukushima Daiichi nuclear power plant accident in Japan in March 2011 and the ensuing discussions focused on lessons learned, particularly at European level, boosted developments in the field of probabilistic safety assessments. It should be noted that no complete assessments covering all hazards up to Level 2 exist anywhere in the world. IRSN and EDF are participating in international activities aimed at advancing the state of the art in this area.

[485] Detection is performed by thermocouples installed in the reactor pit.

As periodic reviews have been carried out, particularly those associated with the fourth ten-yearly outage of the 900 MWe units, EDF has added the most plausible internal and external hazards to its reference probabilistic safety assessments, based on the state of the art concerning methods and the availability of appropriate data.

IRSN, for its part, continues to develop probabilistic safety assessments, aiming to obtain the knowledge and information required during periodic reviews to allow the Institute to give its opinion on the validity of the conclusions drawn by EDF's probabilistic safety assessments and to determine whether modifications proposed to improve facility protection against hazards are satisfactory.

14.5. Using probabilistic safety assessments

14.5.1. Using PSAs in the design phase

14.5.1.1. Usefulness and particularities of PSAs in the design phase

When the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors were written in the 1990s (see Chapter 18), the state of the art called for a simplified PSA at the design stage, including certain probabilistic targets.

In this regard, the technical guidelines state that:

- "a probabilistic safety assessment must be conducted from the outset of the design stage and must include at least internal events; this probabilistic safety assessment should indicate the frequency of core-melt sequences, and also provide a view of the possible consequences that the different core-melt situations could have on the confinement function";
- "implementation of improvements to defence in depth on these plant units should make it possible to achieve a total core-melt frequency of less than 10^{-5} per year per reactor, taking into account uncertainty and all types of failures and hazards";
- "to determine the adequate combination of redundancy and diversity in safety systems, the designer can use probabilistic targets as guideline values; in this case, guideline values of 10^{-6} per year for the probability of core melt due to internal events respectively for power states and shutdown states could be used, bearing in mind the need to consider any associated uncertainties".

Since these technical guidelines were published, the state of the art regarding probabilistic safety studies has evolved. Consequently, EDF conducted a Level 2 PSA for commissioning of the Flamanville 3 EPR.

Probabilistic safety assessments conducted in the design phase generally contribute the following benefits:

- they substantiate the design of safety systems, particularly when choosing suitable measures in terms of redundancy and diversification, allowing different design options to be assessed and compared;
- they provide an assessment of the total frequency of core melt and the frequency of any release, which is useful to assessing safety at the design stage and measuring progress made with regard to previous reactors;
- they confirm that a balanced design has been achieved in terms of reactor safety, i.e. there are no scenarios that make an excessively large contribution to the total frequency of core melt;
- they contribute to the assessment of facility robustness with regard to hazards, when appropriate PSA models and the necessary data are available;
- they provide support when verifying that appropriate measures have been taken to reduce the frequency or mitigate the risks of events corresponding to multiple failures;
- they substantiate that appropriate measures have been taken to reduce the frequency or mitigate the risks of core-melt accidents;
- they may contribute to substantiating the 'practical elimination' of sequences that could lead to large early releases.

The extent of these contributions obviously depends on the scope covered by the PSAs used.

As pointed out in the technical guidelines mentioned above, the results of PSAs performed at an early stage of design must nonetheless be used with caution. The specific characteristics of these studies (functional analyses of accident scenarios limited by the level of detail in the information available on facility performance, equipment reliability data generally compiled from generic databases, simplified probabilistic human reliability analysis in the absence of exact knowledge of the accident operating procedure, etc.) imply that there are major uncertainties in the results.

Although comparison of the PSA results with quantitative probabilistic targets can provide useful information, it should be emphasized that these probabilistic targets are not considered to be acceptance criteria in French practice.

14.5.1.2. PSAs conducted to support the Flamanville 3 EPR design

▶ Level 1 PSA

The Level 1 PSA for the Flamanville 3 EPR was developed in stages as reactor design progressed. The first studies were conducted by the designer from the outset of the design phase and were then updated quite regularly. They were enhanced as facility design advanced and more accurate information became available, particularly with regard to accident studies and operational tasks.

At the beginning of the design stage, the Level 1 PSAs conducted by the designer were limited to internal initiating events. Additional hazard assessments were added later. PSAs were thus developed (in the early 2010s) for fires, flooding and explosions originating inside the facility. For external hazards, the information provided was generally qualitative, with probabilistic information used mainly for hazard frequency.

An analysis of the results of the first assessments – some of which pre-dated the application for construction authorization – led to several facility improvements. These included diversification of the cooling pumps for the low-pressure safety injection system, diversification of the automatic startup signal of the RCS water makeup if cooling is lost when the reactor is shut down, and diversification of the spent fuel pool cooling system, with the creation of a third diversified train.

Further assessments, carried out in particular when applying for construction authorization and operating authorization for the Flamanville 3 EPR, confirmed the benefits of these changes and provided additional information, which led to further design and operation modifications, such as:

- in the event of an accident situation caused by a loss of off-site power, the use of interconnections between electrical trains originally provided for maintenance purposes,
- changes to the design and operation of certain ventilation systems in order to reduce the calculated frequency of core melt resulting from situations associated with the failure of these systems (diversification of the chillers in the safety chilled water system and the reactor building chilled water system, which provide cooling for the electrical building main ventilation system; prohibiting maintenance on a main ventilation system train when the outside temperature is above 25°C, etc.).

▶ Level ‘1+’ PSA

To push assessment of the EPR design with regard to the objectives set out in the technical guidelines – which were not effectively valid until the ASN sent them to EDF in 2004 –, especially to achieve the goal of ‘practical elimination’ of core-melt accidents that could lead to large early releases, the designer produced the first extended version of the Level 1 PSA (known as the Level 1+ PSA), to assess effects on the containment. The accident sequences leading to core melt in the Level 1 PSA were grouped together on the basis of certain parameters (physical parameters, containment state, etc.), then ‘categorized’ according to the success or failure of actions taken to mitigate the subsequent risks (operator depressurization of the reactor coolant system, availability or unavailability of the containment heat removal system [CHRS][486], success or failure of containment isolation).

Three main categories of plant damage states (PDS) were defined:

[486] The heat removal system for the EPR containment.

- category PDS 1, consisting of the core-melt sequences for which risk mitigation systems are available;
- category PDS 2, consisting of the core-melt sequences leading to long-term containment failure (such as sequences in which the CHRS is unavailable);
- category PDS 3, consisting of the core-melt sequences leading to early containment failure.

This first assessment revealed that the frequency of sequences leading to core melt with the CHRS system unavailable was relatively high because of the support systems common to the core-melt prevention systems and the risk mitigation systems. The designer then decided to diversify the cooling system and the power supplies to the CHRS by installing additional dedicated cooling pumps powered by the two 'small' generators provided in addition to the four main diesel generators (see Section 18.2.3.). An update to the Level 1+ PSA confirmed the benefits of these changes.

Following updates of the Level 1+ PSA by EDF, it soon became clear that a Level 1+ PSA would not take into account sufficient details on equipment characteristics, the physical phenomena involved in core-melt accidents and their chronology to provide an accurate assessment of containment behaviour during these accidents and the associated risks of releasing radioactive substances into the environment.

For this reason, in 2000 EDF decided to develop a Level 2 PSA for the Flamanville 3 EPR, within the deadline for submittal of the safety analysis report provided when applying for the operating authorization.

▶ Level 2 PSA

EDF therefore developed a Level 2 PSA to accompany its application for the Flamanville 3 EPR operating authorization. This assessment contributed considerably to demonstrating that appropriate measures had been taken to manage a core-melt accident. It also provided additional information for accident situations that were beyond the EPR design basis, such as long-term loss of power supply and loss of coolant. This information was used to define complementary measures for managing these accidents, to be implemented by the Nuclear Rapid Response Force (FARN) developed by EDF after the Fukushima Daiichi nuclear power plant accident.

At a later time, this Level 2 PSA will be updated to reflect final reactor design (engineered safety systems, risk mitigation systems, operating procedures and so on).

14.5.2. Using PSAs in periodic reviews

A specific periodic review process is carried out for each particular reactor type, taking into account operating experience and growing knowledge in reactor safety. The review consists of (see Chapter 30 for further details): a compliance study of the reactor with applicable requirements, and the search for safety improvements that will bring the reactor series into line with more recent reactors (the safety reassessment). These two parts are a regulatory requirement.

14.5.2.1. Level 1 PSA

PSAs are generally used during periodic reviews to reassess total core-melt frequency, to apprehend how it has changed in relation to the assessment carried out during the previous review, taking into account operating experience feedback and new knowledge, and to determine the main contributions to total core-melt frequency. This process is used to identify any relative weaknesses of the facility for which changes to both design and operation could be investigated or could actually be considered as necessary. Weaknesses are ranked to indicate the order of priority in which they are to be addressed.

Level 1 PSAs are also used during periodic reviews to define complementary measures (for events characterized by multiple failures). This specific use is explained in Chapter 13.

In practice, at the beginning of a periodic review of a reactor series, EDF updates the corresponding reference PSA established for the previous review, incorporating the most recent operating experience (updating the list of initiating events and their frequency, as well as equipment reliability data and operating profile) and any new knowledge about facility behaviour in light of the most recent studies.

To identify and rank the main contributions to total core-melt frequency, elementary sequences with similar characteristics in the event trees are grouped together as 'functional sequences', then the core-melt frequency associated with each functional sequence is assessed. The purpose of this grouping process is to determine functional sequences for which the frequency and consequences could be reduced by implementing a single measure, in order to identify improvement opportunities more effectively.

At the end of the periodic review, a new version of the reference PSA is produced by EDF, taking into account the modifications decided on during the review.

IRSN uses its own PSA models for its assessment purposes. Its approach consists in:

- examining the pertinence of the input data used in EDF's assessments (reliability data, independent failures and common-cause failures, frequency of initiating events, etc.),
- identifying and analysing the main differences between the PSAs submitted by EDF and those developed by IRSN before the review, in terms of assumptions, modelling choices, PHRAs and results,
- carefully examining the functional sequences of particular interest in terms of safety.

During the IRSN assessment, discussions are held with EDF regarding possible improvements to facilities and facility operation (operating procedures) and ways in which EDF's PSAs could be improved.

Although Level 1 PSAs relevant to internal events had already been used extensively in the framework of the second ten-yearly outage on 900 MWe units, it was only from the second ten-yearly outage of the 1300 MWe units that the use of PSAs was made systematic and effectively 'enacted'.

During the following periodic reviews, this approach was consolidated and also enhanced by extending the scope of the PSAs, as EDF took on the following tasks:

- an Internal Events Level 1 PSA for the spent fuel pool and an Internal Events Level 2 PSA for the third ten-yearly review of the 900 MWe and 1300 MWe units,
- Fire and Internal Flooding Level 1 PSAs for the third ten-yearly review of the 1300 MWe units,
- Internal Explosion, Earthquake and External Flooding Level 1 PSAs, Fire, Internal Flooding and Earthquake Level 2 PSAs for the fourth ten-yearly review of 900 MWe units.

These PSAs led to the adoption of design and operating improvements at the time of the different periodic reviews. In particular, the Internal Events Level 1 PSAs led to more in-depth examinations during the third ten-yearly review of the 900 MWe and 1300 MWe units with regard to sequences leading to core melt with containment bypass, induced by a rupture of the coil in the thermal barrier of a reactor coolant pump. If isolation of the section of the component cooling system designed for the reactor coolant system operating conditions fails, this type of rupture can lead to a reactor coolant system break outside the containment, with no means of isolating the break or restoring the pressure and temperature conditions that would make it possible to stop the flow of water from the break. The operator decided to improve the means of isolating the component cooling system and updates of the PSAs confirmed the benefits of this change.

The Fire PSA conducted by EDF for the third ten-yearly review of the 1300 MWe units identified a high frequency of sequences leading to core melt induced by fire in a room containing cabinets for the computerized relays (Controbloc) of the instrumentation and control system, which could lead to inadvertent opening of the RCS protection valves and impair reliability of the safety injection and containment spray systems required to mitigate the risks entailed by the situation. In view of this, EDF decided to modify the control logic of these valves.

14.5.2.2. Level 2 PSA

Level 2 PSAs are used during periodic reviews to assess the benefits and opportunity of making improvements to equipment (particularly on existing systems) and procedures, with a view to reducing the probability of containment failure modes or mitigating the risks of such failures in terms of release. These assessments may contribute to the design and installation of systems used to prevent core-melt accidents or mitigate the corresponding risks, and can also serve to improve the severe accident operating guidelines.

The first time Level 2 PSAs were used in a safety analysis was for the third ten-yearly review of the 900 MWe units. Now, for each periodic review, EDF carries out a Level 2 PSA reflecting the reactor condition before and after the changes made as a result of the review. These PSAs serve to identify and mitigate as far as reasonably possible the risks presented by the reactors. For the 900 MWe, 1300 MWe and 1450 MWe units, general objectives are set for each review in the 'severe accident baseline'. In the case of the third ten-yearly review of 900 MWe and 1300 MWe units, the main objective was to mitigate the risks of large early releases. During subsequent reviews, the aim was to bring the safety level of the reactors in operation closer to that of the EPR (discussed further in Section 30.5).

Examples of the use of Level 2 PSAs and ensuing reactor modifications are presented in Section 14.3.3.

Level 2 PSAs can also help to set priorities for research programmes that aim to achieve a better understanding of core-melt accidents and how to mitigate the associated risks.

14.5.3. Using PSAs for reactor operation

14.5.3.1. Using PSAs to analyse event severity

PSAs are used as part of the overall process of analysing operating experience (see in particular Chapter 21, which discusses operating experience practices and rules).

Significant events (a concept explained in Section 21.4) that occur at nuclear power plants are one of the main sources of operating experience feedback. In addition to the standard methods applied in event analysis, Level 1 PSAs can be used to assess the increase in the probability of core melt induced by a real event. This method[487] has been in use in France since the early 1990s.

The probabilistic approach is important for two reasons:

- analysis of the potential consequences of an event is based on an investigation that is as systematic and realistic as possible, covering potential scenarios that describe degradation of the situation created by the relevant event, thereby making the study more exhaustive;
- the probabilistic assessment also provides quantitative information on the probability of these scenarios.

Probabilistic analysis provides figures, which give a clearer picture of the severity of events, making it possible to rank them according to their conditional probability of core melt.

[487] Also referred to as the 'precursor' method (i.e. precursor of core melt), a method discussed further in Section 21.4.

It also helps with setting priorities for dealing with events and assessing the pertinence of actions based on operating experience and the effectiveness of corrective measures.

▶ Definition of 'precursor' events

The severity of an event can be quantified by determining a value known as the 'core-melt probability increase' (or potential risk index, PRI), which is the difference between the conditional annual probability of core melt (keeping in mind that the event has taken place) and the total annual probability of core melt established in the reference PSA model. Events with a PRI greater than 10^{-6} are called 'precursors', which are subject to more in-depth analysis. Among these events, those with a PRI greater than 10^{-4} receive special attention: the operator defines corrective measures and sets deadlines for their implementation. The expected gains from implementing these corrective measures is assessed probabilistically, if possible.

▶ Probabilistic analysis

EDF and IRSN each carry out their own examination of significant events that occur in reactors when these events are reported. This examination identifies any key events, some of which could be precursors as defined above.

When a key event has been identified, if possible, an assessment is conducted to determine any increase in the probability of core melt in relation to the event. However, this method cannot be applied to all events because of the limitations of the Level 1 PSAs carried out by IRSN and EDF.

There are two categories of precursor events:

- those resulting from an equipment failure or unavailability that could lead to the degradation of one or more engineered safety functions; where degradation of this type could affect the progression of several foreseeable accidents, it is the sum of the annual core-melt probabilities of the corresponding accident families that represents the increase in annual core-melt probability for the event;
- those referred to as pre-initiating events: for this type of event, it is the annual probability of causing an initiating event (in the sense of PSAs) that is used to derive the associated core-melt probability.

Some events meet both of the above definitions. In this case the increase in the annual core-melt probability in relation to the event is calculated taking into account both aspects.

In general, analysis is conducted using the reference PSA model and no particular development is required. However, sometimes the PSA model must be adapted to the specific characteristics of the event, which is the case for any state of unavailability affecting the reactor at the time of the event.

If the event is due to an equipment failure, an assessment should be made to determine whether the failure could affect other systems or components and the associated assumption should be included in the quantification.

If significant uncertainty is associated with the quantification assumptions, a sensitivity study must be conducted.

14.5.3.2. Using PSAs to analyse operational limits and conditions and temporary changes

The general purpose of operational limits and conditions (OLCs, see Section 20.2) is to define a set of rules that must be complied with during (normal) operation of the facility to keep the reactor within the domain covered by the safety analysis report.

Operational limits and conditions define:

- the different operating domains of the facility, characterized by bounding values for physical parameters,
- the functions, systems and components that must be available in each operating domain to prevent and detect incident and accident situations and mitigate the risks if these situations should nonetheless occur,
- the actions to be taken if there is a deviation from the requirements mentioned above, and the maximum time allowed to take these actions.

The operational limits and conditions for reactors were written using a deterministic approach, based mainly on the studies of design-basis accidents covered in the safety analysis report, along with expert opinions.

Over time, the use of probabilistic safety assessments has made it possible for EDF to define lasting changes to the operational limits and conditions, particularly for shutdown states. These probabilistic assessments can also be used by EDF and IRSN to analyse temporary changes to these specifications.

A brief list of the main areas in which EDF currently uses its PSAs to define operational limits and conditions is given below. IRSN's analyses mainly concern the methods chosen by the operator and the assumptions made when applying these methods. IRSN also applies the following precautions when using PSAs:

- a verification is made to ensure that the PSA used is appropriate for assessing the case in question, which can sometimes lead to other specific studies; certain simplifications in the PSA may, in fact, prove to be inappropriate for the use in question;
- another verification is conducted to ensure that the conclusions of the assessment take into account the limitations of the PSA level (1 or 2)[488] and the corresponding scope of assessment;

[488] For example, a Level 1 PSA is not appropriate for assessing unavailability of equipment related to the containment.

- regardless of the results of the probabilistic assessments, calculation of the maximum time for equipment repair or achieving reactor fallback must take into account real-life maintenance imperatives (the actual time required for repair) and operational requirements (the actual time required to prepare for fallback). The verification of compliance with deterministic criteria is also essential (for example, if the duration of system or component unavailability compromises an assumption posed in the design-basis accident study, then the duration of unavailability in the PSA must be strictly limited).

▶ Defining the safety functions and equipment that must be available for a given reactor state

Before stating in the operational limits and conditions that a particular system or component must be available in a given reactor state, it may be of interest to consider the cost or benefit of this requirement by assessing the increase in total annual core-melt frequency that would result if the system or component were to be unavailable throughout the duration of that state.

▶ Classifying unavailability as a Group 1 or Group 2 event

The unavailability of any system or component required by the operational limits and conditions for a particular reactor state is classified as a Group 1 or Group 2 event, depending on the importance to safety of the system or component in question. A strategy for fallback to a safer state and very strict rules on event combinations are associated only with Group 1 events.

PSAs can provide insight for classifying unavailability events, particularly in the case of systems and components that play an important role in the case of multiple-failure events (Chapter 13).

▶ Defining operating procedures in the case of a Group 1 event

PSAs provide clarification as to the best operating procedure to be followed if equipment required by the operational limits and conditions is unavailable, in terms of the actions to be performed and the maximum time allowed to take these actions. Other factors still need to be considered for decision-making, such as the impossibility of repairing equipment in a given reactor state.

A method based on an approach that is both probabilistic and deterministic was developed through discussions between EDF and IRSN to define the most appropriate operating procedure for unforeseen events in Group 1, namely fallback to a safe state within a certain time period or repair in the initial state. Compensatory measures are necessary if the total annual core-melt frequency due to unavailability is relatively high.

▶ Role of PSAs when assessing temporary changes to operational limits and conditions

PSAs can also be used in addition to deterministic analyses, by both EDF and IRSN, when assessing requests for temporary changes to the operational limits and conditions, authorizing the facility to operate outside the domain defined in the OLCs.

The purpose of probabilistic analysis is to check that, taking into account the corrective measures implemented by the operator, the increase in the total annual core-melt frequency remains low throughout the temporary change to the operational limits and conditions (a value of 10^{-7} per temporary change is used as the benchmark).

A substantiating probabilistic analysis may accompany the operator's request, or may be called for by IRSN during its technical review of the request. IRSN checks its pertinence based on the information sent by the operator, in particular using its own PSA models.

14.5.3.3. Using PSAs to analyse operating procedures

Although probabilistic information is not systematically required to substantiate procedures used in incident and accident operation, PSAs by EDF and IRSN are used as investigative tools to analyse these procedures. They provide a particularly useful contribution when the time window for performing certain required actions is short. In this type of situation, regardless of the PHRA model used, the probability of operator failure is higher than that of the failure of an automated system performing the same function. Estimating the core-melt probability associated with the sequences concerned is useful for deciding whether automation is required. PSAs have provided conclusive information for addressing certain issues important to safety, such as the risk of cold overpressure induced by an RHRS break in states where the RHRS is connected to the reactor coolant system. Initially, EDF made improvements to the operating procedures, but the high core-melt frequency still associated with this type of sequence and the uncertainty of sequence modelling caused EDF to make a physical change as well, which consisted in adding a pressure relief device to limit overpressure.

More generally, analysis of operational documents regularly shows that particular situations, such as combinations of low-probability failures, are not covered in these documents. IRSN examines the benefits of including them in these documents, taking into account the added complexity that this might bring to operation, or even to the facility. In this context, the results of PSAs can provide useful information.

Chapter 15
Aspects Specific to PWR Spent Fuel Storage Pools

The spent fuel storage pool (more accurately the spent fuel assembly storage pool) is located in the fuel building (FB) of French PWR nuclear power plants (see Figure 15.1). It is used to store spent (irradiated) fuel until its decay heat decreases enough to allow removal of the fuel from the site (radioactive decay pool). It also serves during reactor outages to temporarily store new or used fuel to be loaded or reloaded for the next operating cycle. Depending on the reactor series, the storage capacity ranges from about 300 to 600 fuel assemblies, reaching up to 1000 fuel assemblies for the Flamanville 3 EPR.

The spent fuel pool cooling and purification system (FPCPS) for 900 MWe[489], 1300 MWe and 1450 MWe reactors has two pumps, each powered by one of the two emergency-supplied electrical trains, and two heat exchangers (the case of the EPR is discussed later). Unlike the reactor coolant system, the spent fuel pool cooling system is not pressurized because it is continuously connected to the pool, regardless of the type of reactor. The design requirement defined for the FPCPS is that, in the event of failure of one of its components (pump, exchanger or others), the pool water temperature must not exceed 80°C, to prevent the water from boiling. The FPCPS is consequently not a 'high-energy' system and when it was designed, a sudden break in the system was considered highly improbable.

[489] Except for the Bugey nuclear power plant reactors, which have three heat exchangers.

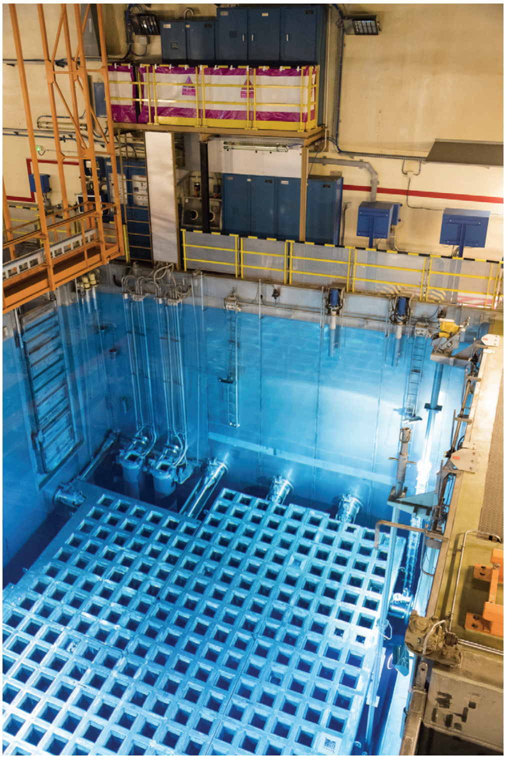


Figure 15.1. The spent fuel pool and its storage racks at the Saint-Laurent-des-Eaux nuclear power plant. Laurent Zylberman/Graphix-Images/IRSN Media Library.

Given the configuration adopted for fuel assembly transfer between the fuel building and the reactor building through the transfer tube, the spent fuel pool service floor is between 20 m and 26 m above the reactor platform, for a storage pool depth between 12 m and 13.7 m. The volume of the storage compartment is greater than 1000 m^3. When the reactor series were designed, the maximum permissible decay heat generation for fuel storage in the compartment was between 5 and 8 MW for the 900 MWe and 1300 MWe reactors and 14 MW for the N4 series reactors[490]. Based on this assumption, in the event of total loss of cooling, it took a long time before conditions that could cause sudden alteration of the fuel (cliff-edge effects) were reached. For the CPY series 900 MWe reactors, the estimated time to pool water boiling was 14 h and the time to stored fuel assembly uncovery was greater than four days, without activation of an emergency water makeup system.

Based on these considerations, the probability of occurrence of a spent fuel pool cooling accident was judged to be low. However, after a few years of operation, significant shortening of the time between reactor shutdown and fuel unloading from the

[490] Envelope values in reactor core complete fuel unloading situations.

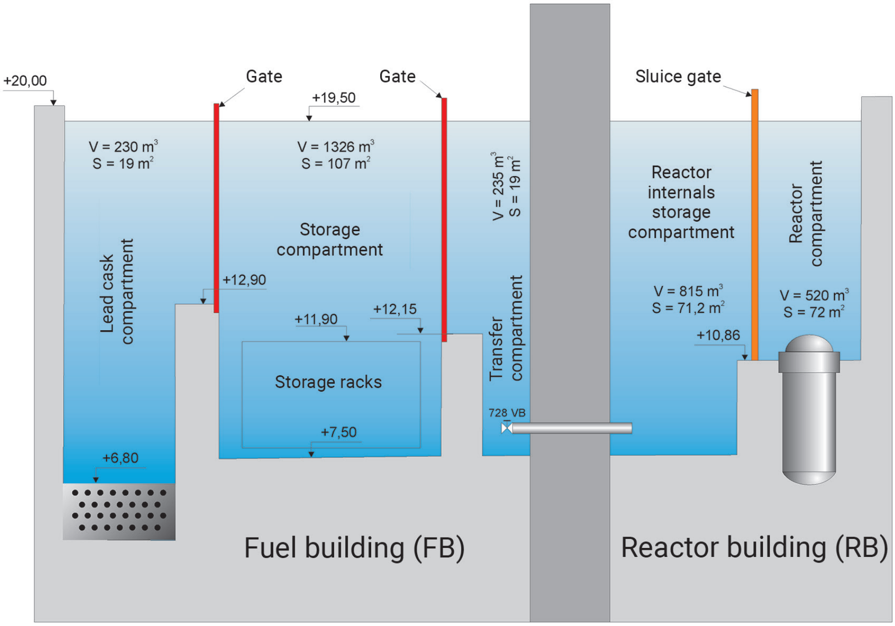
core led to an increase in the decay heat of the fuel stored in the pool on completion of unloading[491]. Over time, it became clear that changes had to be introduced in the initial design to improve the safety level of the spent fuel storage pools.

It is noteworthy that since the startup of the various French nuclear power reactors, there has not been a single case of personnel being exposed to irradiation in connection with spent fuel storage pools.

15.1. Spent fuel pool design

15.1.1. Confinement barriers

The spent fuel pools of the French pressurized water reactors (see Figure 15.2) are located outside the reactor containment[492], and the fuel building (FB) that houses them is not subject to a leaktightness requirement. However, the pools are kept under dynamic confinement provided by ventilation systems which, in normal conditions, keep them at negative pressure and also filter certain radionuclides in the event of an incident or accident by means of high-efficiency particulate arresting (HEPA) filters and iodine traps.



Georges Goué/IRSN

Figure 15.2. Section through the reactor building (RB) and fuel building (FB) of a CPY series 900 MWe reactor, showing the various compartments.

[491] Increased burnup also had an effect on this increase in decay heat.

[492] For the EPR, the aeroplane crash (APC) shell covers the fuel building but does not confine radioactivity released inside the building.

Three confinement barriers are involved in underwater storing and handling of irradiated fuel:

- the fuel rod cladding;
- the water around the fuel rods (which retains non-gaseous radionuclides in the event of cladding damage), the concrete structures and the leaktight pool liner, which constitute physical 'barriers' at the sides and bottom of the pool;
- the fuel building dynamic confinement and filtration system.

However, an accident resulting in boiling of the water or draining of a compartment containing spent fuel could entail more or less rapid loss of the water and eventual damage to the cladding exposed to air.

Moreover, vaporization of a large quantity of water in the event of pool overheating would lead to shutdown of the extraction and filtration systems of the fuel building ventilation system. Dynamic confinement would consequently not be maintained. To avoid transfer of water vapour to the various spaces inside the fuel building (which would particularly interfere with action taken to make up the water level in the pool), the hall above the pool service floor would then need to be opened to the outside environment to create an outlet.

Consequently, the fuel building confinement would be fully operational only in certain accident situations compromising fuel assembly cladding integrity, such as handling accidents. Under other conditions, the radiological consequences of uncovery of one or more fuel assemblies, which would result in the melting of the fuel, could not be sufficiently mitigated by this confinement configuration. Furthermore, fuel melting in this scenario could be accompanied by energy-generating phenomena, such as an explosion of the hydrogen produced by fuel assembly cladding oxidation, which could blow away the upper part of the fuel building or cause a zirconium fire.

Fuel assembly melting in the fuel building is consequently an accident that could entail very substantial radioactive release to the environment. 'Practical elimination'[493] of this type of situation is therefore necessary, which is indicated explicitly in the technical guidelines applicable to the EPR (see Section 15.5).

15.1.2. Initiating events defined at the design stage

As discussed in the introduction to this chapter, the spent fuel pool cooling system of the nuclear power reactors (excluding the EPR, which is covered further on) was designed in compliance with the single-failure criterion for certain equipment, and features two pumps and two heat exchangers. The applicable requirement is that, if one of these components fails, the pool temperature must not exceed 80°C. Taking into account an aggravating event independent of the initiating event, using the same safety approach as that applied to the reactor, would lead to pool water boiling (for example, assuming failure of the second cooling system pump when an initiating event

[493] See sections 8.2.2 and 17.10.2.

has led to failure of the first pump). The thermal inertia of the pool, however, was estimated to be sufficient to allow enough time to recover a cooling train before the water temperature would exceed 80°C.

Moreover, as the pool cooling system is not a ‘high-energy’ system, pipe break initiating events likely to lead to rapid draining of the spent fuel pool were not taken into consideration.

Consequently, no emergency water makeup system was provided to compensate any drop in the pool water level due to evaporation or loss of integrity of a system connected to the pool. Similarly, no dedicated automatic control system was installed to isolate a leak automatically if a drop in water level was detected. Furthermore, the layout of the pipes connected to the spent fuel pool was not specifically examined in the design studies with a view to averting fuel assembly uncovery during handling in an accident situation, handling taking place under a much lower depth of water than the water depth above the stored fuel assemblies. It should also be noted that the resistance of equipment contributing to pool leaktightness, such as the water cooling and purification system pipes and the leaktight metal liners of the compartments, was not verified for resistance to thermal stresses generated by a water temperature above 80°C.

Operating experience feedback showed that the potential for pool accidents deserved to be better analysed. The next sections describe how improvements to spent fuel pools were gradually introduced.

15.2. Experience feedback

15.2.1. Loss of cooling

15.2.1.1. Loss of heat sink

Operating experience from pressurized water reactors in the French nuclear power plant fleet has shown that an external hazard could cause total loss of the heat sink for the reactor and the spent fuel pool.

The winters of 1985, 1986 and 1987 included periods of sustained cold with several occurrences of very significant flow slowdown in the cooling systems due to the formation of ice shelves or piling up of ice blocks at the water intakes of nuclear power plants on the banks of the Loire River[494].

Extreme cold episodes of this type can also result in icing on specific equipment items such as the water intake protection grilles, resulting in an exceptional pressure drop. This phenomenon, called ‘frazil ice’, can also obstruct the water intakes of cooling systems.

[494] An example is given in Section 23.3.

More generally, operating experience has shown that there are many potential causes of total loss of the heat sink associated with a reactor and its pool, or a site: examples include a massive arrival of clogging materials in the form of plants[495] (such as algae and branches), animals (such as sea gooseberries), drifting hydrocarbon slicks, or gradual silting of the water intake, to name a few. This feedback has revealed that the frequency of such events is significant and that they may last for some time (requiring several days to restore cooling).

This operating experience feedback led Électricité de France (EDF) to include a potential total loss of spent fuel pool cooling over a period of four days in its general reassessment of fuel-storage-pool design conducted in the early 2000s. This situation now constitutes a design extension condition (see Chapter 13) used to verify the design of systems required to allow the facility to reach and maintain a safe state.

15.2.1.2. Risks related to maintenance during unit outages

Unit outages, particularly when they include complete fuel unloading from the reactor, are the most favourable periods for servicing, maintenance and modification of the facility (other than in the pools). Many systems, including electricity distribution or instrumentation and control, may be partly or totally unavailable during outages. However, during these outages, decay heat from fuel stored in the fuel building pool is at its highest.

At the design stage, no provision was made for redundancy (by electrical train B) of the train A instrumentation that controls pool parameters (water temperature and level, dose rate on the service floor). This means that the fixed monitoring devices could be unavailable during preventive maintenance work on the train A electrical switchboards during unit outages.

Similarly, the fuel building ventilation system used in normal operation is powered by electricity distribution train A; maintenance work on train A may require switching the fuel building ventilation over to the emergency system, which has a much lower flow rate (three to five times lower for the 900 MWe and 1300 MWe reactors). Experience has provided evidence of potential water mist formation in this situation, because of the relatively high temperature of the pool water (about 50°C). Apart from the inconvenience for floor operators, this high humidity could reduce the effectiveness of the iodine traps if the heaters upstream were unable to fulfil their function completely.

Lastly, electrical switchboard shutdowns may lead to unavailability of one of the two pool cooling system pumps. This reduces the reliability of the cooling function.

Several measures were adopted during the general reassessment of fuel storage-pool design mentioned above and implemented during unit outages or as part of modification work packages carried out during ten-yearly outages. They aimed to lower the probability of total loss of pool cooling or loss of confinement efficiency during a unit outage, for example by ensuring redundancy (using both train A and train B) for the

[495] An example is given in Section 24.2.

instrumentation that monitors pool parameters, along with other measures that were more organizational.

15.2.1.3. Suction of foreign matter into the cooling system

An operating experience report produced in 1996 showed that a dozen or so events due to foreign matter in the FCPCS cooling system had occurred since the first French nuclear power reactors were commissioned. Diverse types of foreign matter were identified (washer, vacuum cleaner, filter basket, metal chain, video camera, foam plug, lamp and others).

As a result, cooling system downtime was sometimes long (10 to 20 h).

To avoid recurrence of such events, in the early 2000s EDF installed a strainer on the intake pipe of the FCPCS system on each unit.

15.2.1.4. Exceeding the decay heat defined in facility design

When the spent-fuel-pool cooling systems were first designed, they were sized taking into account partial core unloading (equivalent to a reload of new fuel assemblies) during refuelling outages; complete core unloading was assumed to be exceptional, during the ten-yearly reactor outages, for example. That assumption soon appeared to be inappropriate for effective operation. In addition to problems in controlling fuel assembly and RCCA handling, keeping part of the core in the reactor vessel makes it forbidden to lower the water level in the reactor coolant system to the primary loop invert[496], an operation required to conduct many inspections. Unloading the entire core during unit outages was consequently recognized as the only possible solution in operational conditions.

In parallel, to shorten unit outage time and increase reactor availability, EDF sought to unload fuel assemblies and transfer them to the spent fuel pool as soon as possible. Consequently, the time between reactor subcriticality (i.e. shutdown) and completion of unloading, set to 14 days in the design assumptions, was gradually lowered to six days.

The operating practices developed for this purpose, different from the assumptions made in the initial design, led to a substantial increase in the decay heat from the spent fuel stored in pools during unit outages. For the CPY series 900 MWe reactors, the decay heat limit for fuel stored in the pool, set initially to 2.75 MW in normal operating conditions (5.45 MW in exceptional complete core unloading situations), was reassessed to 10 MW. EDF, in 1994, submitted to the French Nuclear Installations Safety Directorate a request for a concession with regard to the safety analysis report, leading to the general safety reassessment of fuel assembly storage and handling in spent fuel pools, mentioned above.

[496] Lowering the water level to the bottom of the inside of the reactor coolant system pipes.

15.2.2. Water losses

15.2.2.1. Gate or sluice gate failures

A notable event involving draining due to loss of leaktightness on the transfer compartment gate (shown in Figure 15.2) occurred on 16 September 1981, affecting Unit 1 at the Tricastin nuclear power plant during its first refuelling outage, when the reactor core was completely unloaded. During this event (see diagram in Figure 15.3), the transfer tube was open and its isolation valve could not be closed (it was immobilized because of work in progress on the transfer trolley). The reactor building pool sluice gate (shown on the left in Figure 15.3) should normally have been stored away, but fortunately it was in place when the event occurred, although its seal was not inflated.

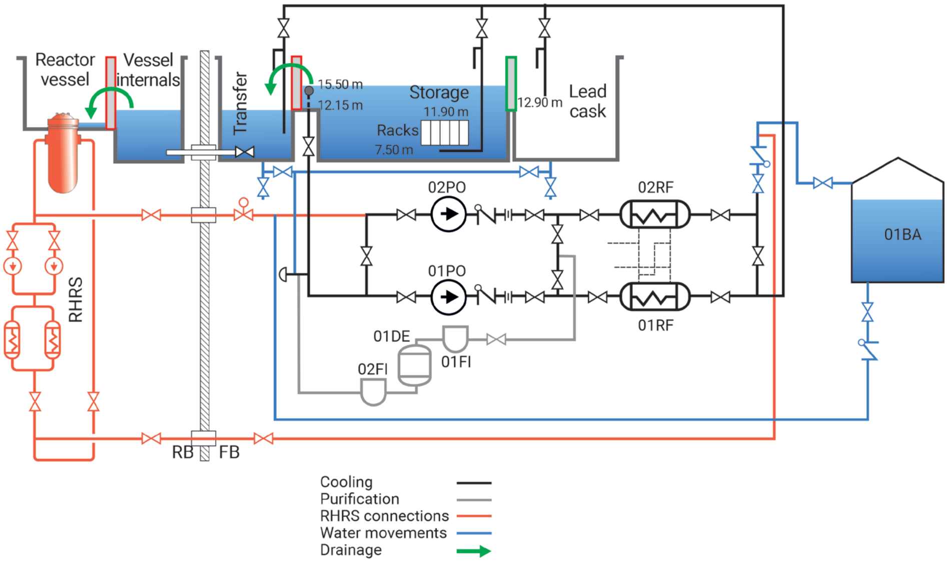


Figure 15.3. Diagram illustrating accidental drainage of the spent fuel pool at Tricastin Unit 1 in 1981. The FPCPS cooling system is shown in black. The refuelling water storage tank (RWST) is on the far right. IRSN.

Draining, at a flow rate of about 10 m^3/h, was caused initially by deflation of the seal on the separating gate between the storage compartment and the transfer compartment following a break in the compressed air control system that normally keeps it pressurized. Subsequent manual resupply of the seal directly by the service compressed air distribution system, not equipped with a pressure regulator, caused the seal to burst, increasing the drainage flow rate to about 100 m^3/h. The drop in the storage compartment water level consequently accelerated. A normally-submerged lamp was uncovered; the lamp and its power supply cable overheated, releasing chlorine vapour. The pool lighting was switched off. The fuel building was then evacuated, leaving one person tasked with monitoring the pool water level.

The plant operator was able to inflate the reactor building pool sluice-gate seal so the drainage could be stopped, balancing the storage compartment water level with the level in the adjacent compartments at 16.5 m, about 6.5 h after the event started. A total of 800 m^3 of water had drained away, but pool makeup during drainage had maintained water above the level at the cooling system inlet pipe, located 4 m below the 19.50 m nominal level of the storage compartment.

Following this significant event and several others, component changes were incorporated to reduce the potential for loss of leaktightness on pool gates and sluice gates:

- pressure gauges were fitted on the inflatable seals of the fuel building compartment gates and the reactor building pool sluice gate, with alarms displayed in the control room in the event of a pressure drop;
- relief valves were installed to protect the inflatable seals against the risk of bursting;
- static lip seals were added to ensure leaktightness of the fuel building compartment gates and the reactor building pool sluice gate, to complement the existing inflatable seals.

15.2.2.2. Line-up errors

French nuclear power plant operating experience shows that a large majority (about 70%) of inadvertent water level drop events in spent fuel storage pools are related to line-up errors.

The resulting draining may occur by gravity or be driven by a pump. Draining flow rates can be high (up to 1000 m^3/h, representing a drop in the water level of more than 1 m in 10 min).

The underlying cause of the observed events is related to the design of the fuel pool cooling system, which has other functions in addition to spent fuel pool cooling. It also backs up the reactor residual heat removal system (RHRS), and its refuelling water storage tank (RWST) is the water reserve for the safety injection system and the containment spray system. The FPCPS also drains and refills the compartments of the fuel building and reactor building pools. The EPR pool is designed differently (see Section 15.5).

Two events, described below, were particularly notable, as they resulted in loss of cooling by the FPCPS following uncovery of its intake pipe located 4 m below the nominal water level in the spent fuel pool (19.5 m).

▶ **The first event** occurred on 18 October 1983 in Unit B2 of the Saint-Laurent-des-Eaux nuclear power plant. The reactor core was completely unloaded and core weld inspections were in progress. As the FPCPS was being lined up, after water makeup in the internal structures compartment (shown in Figure 15.2) of the reactor building pool, the return line to the refuelling water storage tank (RWST) located on the discharge side of the operating coolant pump was opened by mistake. The spent fuel pool was drained to the RWST. The alarm reporting tripping of the pool skimmer pump was activated, followed by the alarm reporting a low water level in the pool.

The operator noted the two alarms but did not realize that they were related to one another. He informed a field operator of the skimmer pump trip and the abnormal water level in the pool, without explicitly asking for an urgent verification. The field operator, occupied elsewhere, did not perform any verification. During shift turnover, the transferred instructions reported the alarms, but since operations were still in progress, no verification was undertaken.

The FPCPS pump in service eventually triggered an alarm due to insufficient water intake pressure. Pool cooling was totally lost by that time. A field operator was sent to the room where the pump was located, but could not clear[497] the fault. He then proceeded to the pool service floor, where he observed that the water level had dropped by about 4 m, uncovering the intake pipe. The pool water temperature increase could not be evaluated, as the sensitive part of the temperature measurement probe had been uncovered during pool draining. The total loss of pool cooling lasted a little over 3 h[498].

▶ **The second event** occurred on 13 February 1986, after refuelling the core of Unit 3 at the Tricastin nuclear power plant and draining the reactor building pool to the refuelling water storage tank using one of the two FPCPS pumps. During FPCPS reconfiguration in spent fuel pool cooling mode, a line-up error resulted in sending part of the circulating cooling system flow to the RWST. The RWST was already full, and consequently overflowed into the concrete retention structure around the tank. This error drained about 500 m^3 of water from spent fuel pool, resulting in uncovery of the FPCPS intake pipe. None of the alarms that could have enabled rapid detection were able to fulfil their function for various reasons – in particular the shutdown of an electrical switchboard, resulting in unavailability of the control room computer, required to display the RWST high water-level alarm.

After detection of the event, when the plant operator attempted to supply makeup water to the spent fuel pool, recovery was impeded by the fact that the main makeup water source, the RWST, was unusable, as the control valves located in the tank retention structure were flooded. Cooling could not be restarted until two to three hours after the event had been detected, and the normal water level in the pool was restored after about 4.5 h. As in the previous event, the pool water temperature increase could not be evaluated. Although, between the two events, a modification had lowered the sensitive part of the temperature probe so that it was still immersed after complete draining, the sensor power supply was cut off due to the electrical switchboard shutdown mentioned earlier.

Another notable draining scenario that emerges from review of operating experience is the potential complete draining of the spent fuel storage compartment by siphoning.

[497] Operation consisting in cancelling an alarm after identifying its origin, in this case with a view to restarting the pump.

[498] The return line valve was closed and pool water makeup was carried out.

Studies conducted in 2002 as part of the first safety reassessment of fuel storage in pools showed that the diameter of the vacuum relief valve on the FPCPS discharge line was too small to stop accidental draining at a high flow rate. On 19 October 1989, a rapid 50-cm drop in the water level of the spent fuel pool occurred on Unit 4 at the Tricastin nuclear power plant (see diagram in Figure 15.4), following a lockout error in connection with preparation for a hydraulic test on the heat exchangers of the reactor residual heat removal system (RHRS).

This event occurred with the reactor core completely unloaded and the reactor coolant system and the RHRS drained. The plant operator had planned to fill the heat exchangers by opening the emergency connection from the FPCPS to the RHRS, and temporary hoses had been installed to connect the heat exchangers to the emergency line. When the valves were opened, a series of alarms were triggered rapidly in the control room, because a valve (RRA 114VB reactor containment penetration), normally locked out in the closed position, was in fact open. In addition to starting draining of the spent fuel pool, this lockout error led to flooding in the reactor building, as most of the RHRS drains were open.

The drainage rate, 'driven' by pump PTR 01PO in service when the event occurred, was estimated at about 300 m^3/h, equivalent to a drop in the water level of approximately 5 cm per minute. Draining continued for about ten minutes until a worker closed a valve on the connection between the FPCPS and the RHRS.

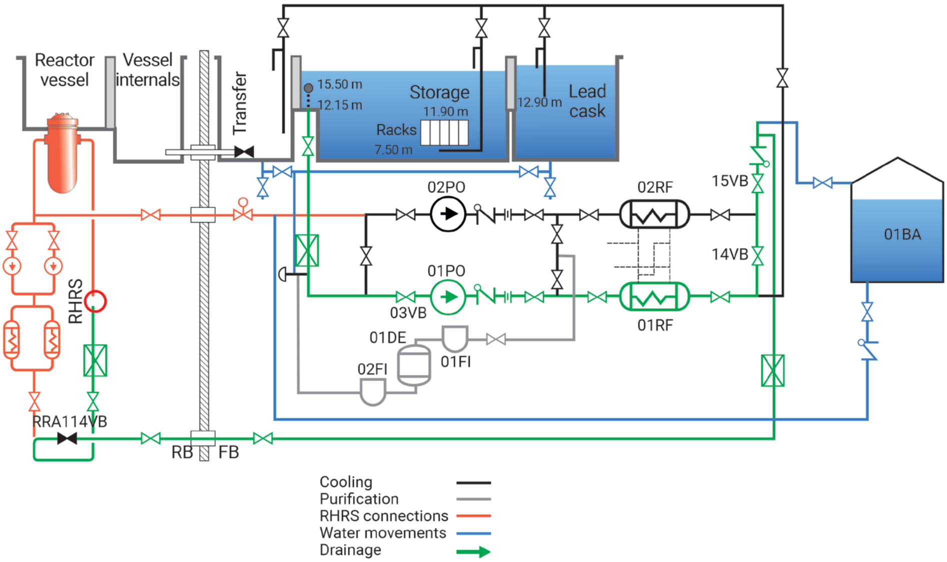


Figure 15.4. Diagram illustrating inadvertent draining on 19 October 1989 after opening valve RRA 114 VB, initially closed (valve shown in black at the bottom left-hand side of the diagram). The red circle represents leakage through the RHRS drains. IRSN.
]

This event could have been much more serious if the lockout error had not been detected rapidly. One of the ways available to operators for stopping a wide range of predictable cases of draining is to shut down the FPCPS pump in service and close the head valve on the intake line of the FPCPS. If this action had been taken by the operating crew, draining could have continued by siphoning (see Figure 15.5) if the discharge line vacuum relief valve did not operate effectively when the FPCPS pump in service was shut down. But this discharge line descends to the bottom of the storage compartment, on the same level as the bottom of the racks. In this case, draining could have led to uncovery of all the stored fuel assemblies.

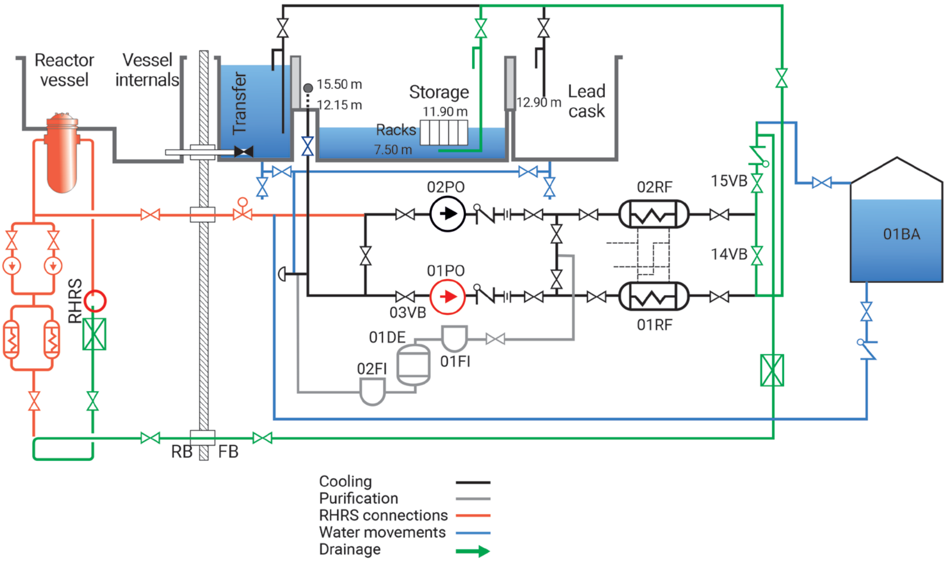


Figure 15.5. Risk that draining continues due to siphoning if pump PTR 01 PO is shut down. IRSN.

Prevention of this type of event has been reinforced by implementation of organizational measures (administrative lockout of FPCPS valves or valves that connect to other systems[499], reinforcement of the operational limits and conditions and the periodic equipment inspections required to detect and stop inadvertent draining). Automatic isolation of the FPCPS intake line, increasing the diameter of the vacuum relief valve on the discharge line of the same system, and systematic redundancy (train A and train B) of water-level instrumentation, also adopted and implemented following the first general safety reassessment conducted on fuel assembly storage and handling in the spent fuel pools (in the early 2000s), contribute to the detection and control of inadvertent pool draining resulting from a line-up error. However, despite these measures, the frequency of line-up errors leading to draining remains significant.

[499] These lockouts depend on the state of the reactor.

Moreover, in the general safety reassessment conducted in the early 2000s, EDF undertook to implement periodic inspections of the vacuum relief valve on the FPCPS discharge pipe to check for any obstruction. However, inspections following the Fukushima Daiichi nuclear power plant accident showed that the FPCPS discharge pipes in Unit 2 and Unit 3 of the Cattenom nuclear power plant were not fitted with vacuum relief valves. This anomaly dated from the commissioning of these reactors (detected on 21 December 2011, it was classified as a Level 2 incident on the International Nuclear Event Scale [INES]).

Despite the above measures, it still remained possible for a vacuum relief valve to fail to operate on accidental draining of the spent fuel pool. Potential solutions included functional diversification of the device (for example by inserting a check valve at the end of the discharge line) or a implementing a design change so that the FPCPS discharge pipe would not drop below the top level of the stored fuel assemblies. EDF decided in 2017[500] to add a check valve to the terminal discharge line of the FPCPS cooling system in order to stop draining in the event of failure of the vacuum relief valve.

15.2.2.3. Failure of a reactor coolant system pipe nozzle dam

During unit outages, nozzle dams with a diameter of approximately 900 mm are installed in the reactor coolant system pipes connected to the steam generators in order to be able to inspect their tubes and complete any necessary repairs during fuel assembly unloading or loading operations. In the event of ‘loss’ of one of these nozzle dams (due to a rupture, for example), the diameter of the resulting break would be equivalent to the diameter of the access manway to the relevant steam generator (about 450 mm). For a CPY series 900 MWe reactor in a refuelling outage with the transfer tube open, the water level drop rate in the reactor building and fuel building pools would be 40 cm/min and, in these conditions, the water level would reach the top of a fuel assembly during handling after a little more than 4 min. The FPCPS inlet pipe would be totally uncovered after about 11 min. After 17 min (see Figure 15.6), the water level would have dropped to the sill of the transfer compartment separation gate (12.15 m, i.e. 25 cm above the top of the fuel assembly storage racks).

This scenario represents the worst-case accident with regard to the risk of fuel assembly uncovery during handling, although ‘rupture’ of the transfer tube between the reactor building and the fuel building would lead to equivalent consequences. Given the drainage flow rate and the calculated time intervals, no measure could avoid uncovery of one or two fuel assemblies during handling (one in the reactor building, the other in the fuel building). These assemblies would overheat and, after a few hours (depending on their decay heat), would undergo sudden and highly exothermic oxidation, which would destroy the assembly skeletons, possibly initiating fuel melt.

[500] As part of the fourth ten-yearly outage of 900 MWe units and the post-Fukushima modifications.

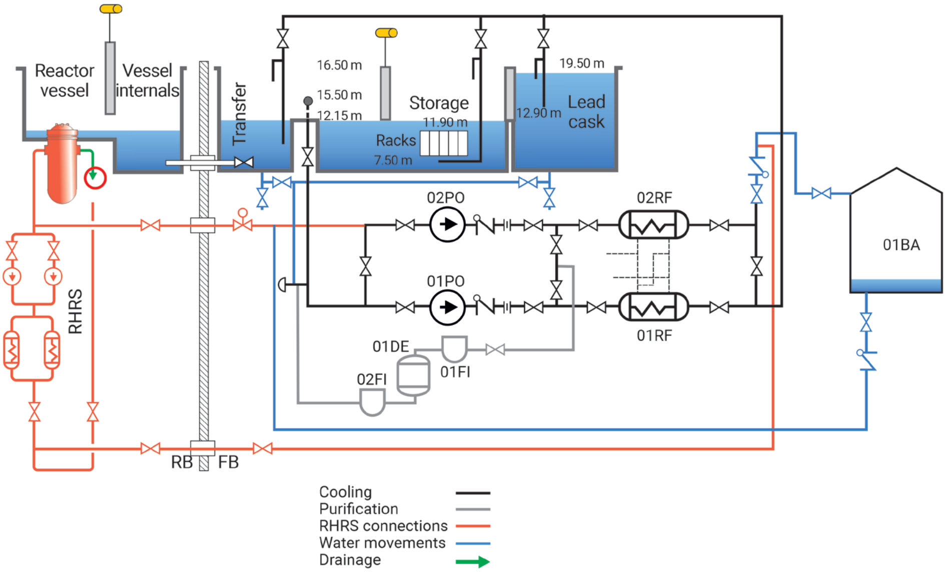


Figure 15.6. Risk of pool draining during outage for fuel assembly handling in the event of 'loss' of a steam generator nozzle dam (water leakage is represented by the red circle). IRSN.

The remaining water in the storage compartment would start boiling after a few hours. The resulting evaporation could be compensated by implementing an emergency makeup procedure using the facility's fire protection water system (the valve station, located at +20 m in the fuel building, would be accessible), but the circulation of fluid in the racks and the consequences of the voids that would be created among the assemblies are poorly understood. Irradiation would be very high at the level of the pool service floor, prohibiting any action at floor level. If an assembly were uncovered in the reactor, the leakage path could not be isolated because of the irradiation, and the assembly could not be placed underwater again (the containment could not be isolated at the transfer tube level in any anticipated scenario).

The reactor coolant system pipe nozzle dams used until 2011 were designed for an operating pressure of 1.3 bars and a test pressure of 2 bars. No accident overpressure load was taken into account in their design.

However, several events involving inadvertent discharge of a safety injection system (SIS) accumulator were observed during fleet unit outages. The SIS accumulators need to be pressurized by the service compressed air distribution system (maximum operating pressure 8 bars) to drain them during maintenance operations. According to studies conducted by IRSN in 2005, SIS accumulator discharge with an air pressure of 8 bars could produce an overpressure wave of approximately 5 bars at a steam generator nozzle dam.

The nozzle dam design has been improved so that it can withstand the predictable accident loads (even at an overpressure of 5 bars). The new nozzle dams are now in use throughout the nuclear power reactor fleet.

15.2.2.4. Rupture of a pipe connected to the spent fuel pool

Although the FCPCS is not a 'high-energy' system, rupture of one of its pipes must be considered. The stresses that might lead to this type of pipe failure could result, for example, from jamming on a pump rotor, a load falling on a pipe, or an earthquake. A significant event in this context involved the installation of biological shielding[501], not designed for earthquake conditions, consisting of lead bricks, in the four units of the Dampierre-en-Burly nuclear power plant, located above the transfer tube; should any of this shielding have fallen, it could have caused the rupture of a pipe connected to a pool. This nonconformity was discovered in 2004 during inspections conducted by EDF during application of the 'earthquake as an event' approach.

Experience also shows that, in some facilities, non-negligible differential settlement of the ground occurred under the reactor building and the fuel building, with an impact on the permissible displacements of the transfer tube in the event of an earthquake. The two buildings are built on different basemats. The transfer tube is secured to the civil works of the reactor building and is also connected to the leak-tight metal liner of the pool in the fuel building. Although the design of the tube and its fastenings allows some displacement of the tube, the differential settlement of the ground under the two buildings reduces permissible displacements in the event of an earthquake.

Operating experience of these events has led EDF[502] to verify the seismic design characteristics of transfer tubes in the relevant facilities, taking into account the observed differential ground settlement. In addition to these studies, a periodic inspection programme was implemented for the transfer tubes[503]. Furthermore, EDF took into account the possibility of an FPCPS main pipe break by resizing the vacuum relief valve of the system for the worst-case drainage flow rate to be considered, doubling the diameter of the valve piping.

15.3. Safety reassessments

As mentioned above, in 1994 EDF applied for a concession to increase the decay heat limit in the spent fuel pools of 900 MWe and 1300 MWe reactors. This led to a general safety reassessment of these pools.

The safety case established for this purpose by EDF between 1996 and 2002 mainly covered the consequences of a spent fuel pool loss-of-cooling incident or accident, and proposed the introduction of a number of improvements regarding prevention, detection and mitigation of this type of situation.

[501] Modification decided by the NPP management, with a view to improving personnel radiation protection.

[502] The measures described were decided before implementation of the post-Fukushima actions.

[503] This inspection programme was required by the ASN as part of the third ten-yearly outage on 1300 MW units and the fourth ten-yearly outage on 900 MWe units. Only a few tubes have been inspected to date.

These measures were based in particular on an operating strategy applicable in the event of total or partial loss of cooling (other than draining situations), for coping with the most pessimistic scenario adopted (loss of the heat sink for 100 h). EDF defined the following objectives in studying this scenario:

- obtain sufficiently low doses at the site boundary, i.e. the doses received as a consequence of release resulting from opening the door of the pool hall that leads to the outside environment in order to avoid pressurization of the fuel building due to pool water vaporization;
- ensure accessibility to the makeup sources and the various rooms in the fuel building, other than the pool hall;
- ensure that the components necessary for management and recovery of a prolonged pool water boiling situation are operational;
- ensure that, when cooling resumes, the FPCPS will only take in subsaturated fluid, a necessary condition for the FPCPS to operate correctly and to return fuel storage in the pool to the safe state;
- ensure leaktightness of the pool gates, sluice gates and the FPCPS at a temperature of 100°C;
- take into account a pool liner leakage rate in an accident situation of 3 m^3/h[504] when sizing the makeup sources and the leakage collection and treatment systems.

The measures introduced following this study (as of 2002) to reinforce the safety of fuel storage in spent fuel pools in the event of a loss-of-cooling accident are practically identical for all the French nuclear power units in operation[505]. They comprise:

- reinforcement and qualification of the pool water level and temperature instrumentation in ambient conditions, while ensuring functional redundancy;
- modification of the FPCPS pipe supports to ensure they can withstand the temperature and ambient conditions prevalent in an accident situation;
- reinforcement of the operational limits and conditions concerning the availability of makeup water sources, the availability of electrical power supplies in the unit outage state, the administrative lockouts to be implemented to avoid draining and other incidents, and reinforcing the FPCPS maintenance programmes;
- as discussed above in Section 15.2.1.3, addition of a strainer at the FPCPS intake in order to avert common-mode loss of the cooling function in the event of foreign matter ingress;

[504] Fixed value taking into account the opening of a certain number of pre-existing defects in the approximately 900 m of welds in a pool liner and the non-leaktightness of concrete structures following a loss-of-cooling accident leading to pool boiling.

[505] For the EPR, the loss of cooling and draining risks were taken into account at the design stage.

- improved reliability in recovering the power supply to the FPCPS pump during work on the electrical switchboards as part of the preventive maintenance operations carried out during unit outages;
- installation of a valve station, accessible even in the event of pool water boiling, so that pool water evaporation losses can be compensated by makeup water from the demineralized water or fire protection systems; the station would remain accessible in the event of fire or flooding;
- reinforcement of isolation between the pool hall and the adjacent rooms (installation of isolation dampers in the ventilation ducts, door modifications, etc.);
- for the 1300 MWe and 1450 MWe units, where the FPCPS is fitted with an intake gooseneck, installation of a makeup line to the pool, designed so that it can also cool the intake line and prevent the formation of a vapour lock that could lead to loss of prime or damage to the pumps or other FPCPS components; modifications have also been made so that the goosenecks can be vented before restarting the pumps;
- establishing an outlet from the spent fuel pool hall to the outside environment (by opening a door or panel) to remove water vapour in an accident situation.

As of 2005 (at the conclusion of studies from the safety reassessment associated with the third ten-yearly outage of 900 MWe units), subsequent periodic reviews have led to close investigation of the potential draining of spent fuel pools, given that the consequences of such draining could be more immediate and more severe than those of total loss of cooling on a pool whose integrity is intact.

The corresponding modifications implemented during the third ten-yearly outage of 900 MWe units – and incorporated in the 1300 MWe and 1450 MWe units as their next ten-yearly outage becomes due (or even before then) – comprise:

- reinforcement of the requirements applicable in normal operation to prevent the possibility of draining and ensure the availability of mitigation means (inspections and periodic tests, maintenance, administrative lockouts, operational limits and conditions), in particular to reduce the risk of line-up errors;
- establishing a specific operating procedure for the case of accidental draining of the fuel building pool or reactor building pool;
- as discussed in Section 15.2.2.3, use of a new type of steam generator nozzle dam, designed to withstand an overpressure of 5 bars;
- sizing the FPCPS discharge line vacuum relief valve for the most pessimistic drainage flow rate to be considered (complete double-ended guillotine break on a main line);
- automatic shutdown of the FPCPS pumps and automatic isolation of the FPCPS intake line if a drop in the water level is detected in the spent fuel pool.

More recently, as part of the modifications planned during the fourth ten-yearly reviews of the 900 MWe units, EDF introduced measures for using fire-service connections to connect an emergency cooling system featuring mobile equipment ('FPCPS 2', see Figure 15.7) outside the fuel building to take over cooling of the spent fuel pool 24 h after the occurrence of a hazard (fire or flooding) that has caused long-term damage to the cooling system. For this purpose, EDF will install a second motor-driven isolation valve on the FPCPS intake line and a check valve on the discharge line.

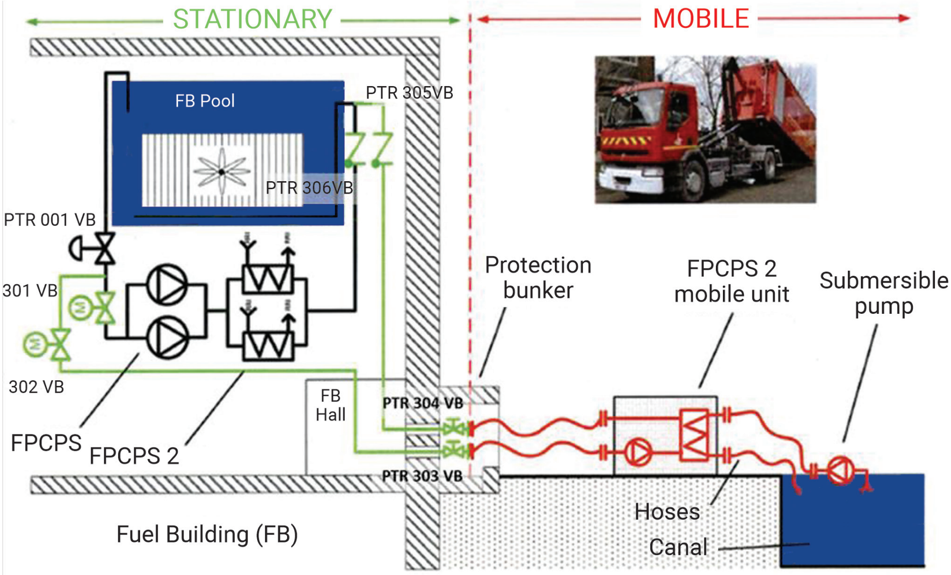


Figure 15.7. Schematic diagram of the 'FPCPS 2' emergency cooling system. IRSN.

15.4. Experience feedback from the accident that affected the Unit 4 pool at the Fukushima Daiichi nuclear power plant

15.4.1. Events

The accident at the Fukushima Daiichi nuclear power plant, featuring six boiling water reactors – following flooding of the site by the tsunami that struck the Japanese coast at 3:40 pm on 11 March 2011 and the resulting total loss of electrical power supplies – is analysed in Chapter 36, which also discusses the lessons learned. The following discussion is limited to the case of the spent fuel pool of Unit 4. When the accident occurred, the core of Unit 4 was completely unloaded; all of the fuel assemblies were in the spent fuel pool, with an estimated decay heat of 2.3 MW.

On 15 March 2011 at 6:10 am, an explosion (attributed to hydrogen) damaged the fifth level of the Unit 4 building (where the spent fuel pool was located), blowing off part of the outer walls of the building.

Early in the morning of 16 March 2011, the plant operator, TEPCO, reported a fire supposedly affecting the north-west corner of the Unit 4 building (the corner where the pool is located), but subsequent messages indicated that there were no longer any traces of fire detected. High irradiation levels were detected near the Unit 4 pool (for example, 400 mSv/h in the access stairways to the upper levels of the Unit 4 building). At about 12:00 am on 16 March 2011, Japanese television broadcast images (somewhat hazy, as they were taken at a long distance, from a helicopter) showing large clouds of steam above Unit 4. At about 6:00 pm (Japan time), the U.S. NRC announced that, according to the information at its disposal, there was no longer any water in the spent fuel pool of Unit 4[506]. On 17 March, in the middle of the day, television channel NHK announced that observations made the previous day by a helicopter in flight over Unit 4 showed that the fuel assemblies were still under water, even though the water level in the pool seemed to be about 3 m below the normal full level.

From 16 to 20 March 2011, no notable event was reported after leaktightness was lost on the gate separating the spent fuel pool and the reactor pool. This gate is self-sealing when the pressure in the spent fuel compartment is higher than the pressure in the reactor pool compartment; the drop in water level in the spent fuel compartment compromised gate leaktightness and water from the reactor pool compartment flowed into the spent fuel pool.

Subsequently, starting on 20 March 2011, substantial volumes of makeup water were transferred into the Unit 4 pool by a pump truck.

The spent fuel compartment of the Unit 4 pool has an area of 120 m^2 and a depth of 11.8 m. Given the fuel decay heat (2.3 MW), boiling of the pool could not have occurred until after about 48 h (i.e. boiling began in the afternoon of 13 March). At that time, the water evaporation rate calculated for adiabatic conditions was less than 80 cm per day. The actual rate observed by the facility operator from 28 April to 5 May 2011, after a deliberate interruption of spent fuel pool water makeup, was about 55 cm per day (see Figure 15.8). However, the level drop given by TEPCO for the period from 14 to 16 March 2011 was faster than these estimates – given that, during this period, water from the reactor pool compartment flowed into the spent fuel pool (see Figure 15.9).

[506] At this point the USA advised their citizens to evacuate the zone within a radius of 50 miles (80 km) around the facility.

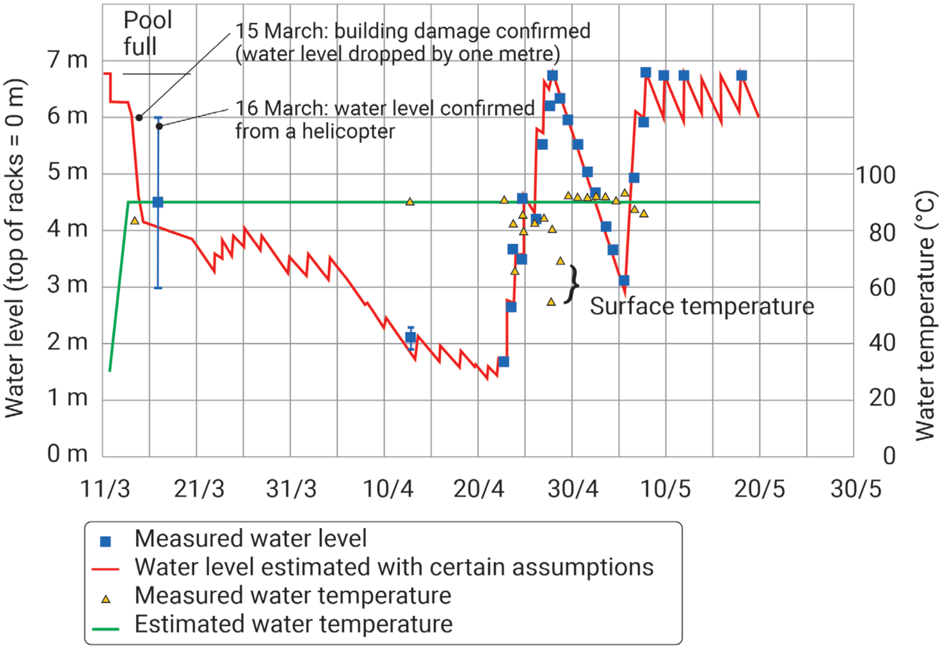


Figure 15.8. Water level and temperature profiles in the Unit 4 spent fuel pool, measured or estimated by TEPCO (from 11 March to 30 May). Tokyo Electric Power Company, Inc. (TEPCO).

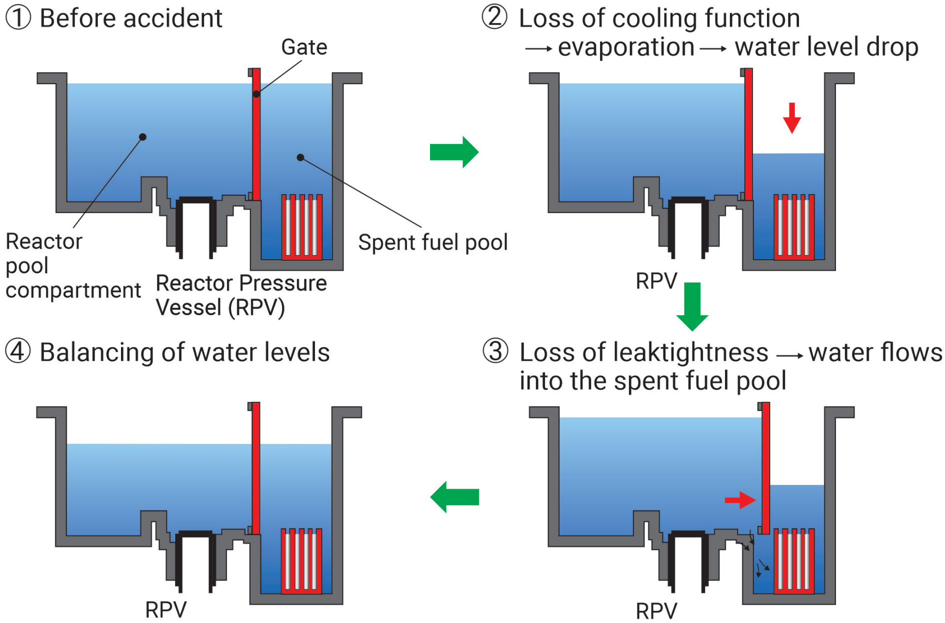

① Before accident
Gate
Reactor pool compartment
Reactor Pressure Vessel (RPV)
Spent fuel pool
② Loss of cooling function → evaporation → water level drop
RPV
③ Loss of leaktightness → water flows into the spent fuel pool
RPV
④ Balancing of water levels
RPV

Figure 15.9. Water flow from the reactor compartment into the spent fuel pool due to loss of leaktightness at the separation between the two pools. Tokyo Electric Power Company, Inc. (TEPCO).

15.4.2. Complementary safety assessments conducted in France

As part of the complementary safety assessments (described in Chapter 36) conducted in France after the Fukushima Daiichi nuclear power plant accident, EDF examined the consequences of an extreme naturally occurring hazard on the systems designed to remove the decay heat generated by fuel stored in pools, specifically a total loss of the heat sink or electrical power supplies, assuming that the integrity of the spent fuel pool was intact. The most pessimistic accident scenario in terms of consequences is a total loss of off-site and on-site electrical power.

In this context, EDF studied measures to be taken in consideration of an extreme natural hazard:

- ensure water makeup in the spent fuel pool by means of an emergency backup system;
- improve operational reliability of the fuel building outlet[507] to ensure that the pool hall can open to the outside environment in a total loss of pool cooling situation;
- provide an ultimate diesel generator to restore the power supply to the ultimate makeup pumping system[508] and to the instrumentation that monitors the pool water level and temperature;
- ensure that a fuel assembly being handled in the fuel building pool can be moved to a safe position using battery-powered means in the event of a total loss of electrical power.

IRSN reviewed these measures as part of the implementation of the 'hardened safety core' concept discussed in depth in Chapter 36. The main question raised by IRSN concerned the assumption of pool integrity in the case of an extreme hazard.

Simplifying somewhat, two cases of accidental pool draining by loss of structural integrity of the pool or of the systems connected to it can be identified:

- draining of the storage compartment, resulting directly in uncovery of the stored fuel assemblies;
- partial pool draining, stopping at the level of the sill of the gates between fuel building compartments (approximately a few tens of centimetres above the top of the fuel storage racks) and, in the reactor building, at the low level of the reactor coolant system pipes.

[507] This outlet avoids pressure build-up in the fuel building and limits propagation of water vapour from the pool hall to other spaces.

[508] This ultimate makeup water would be obtained by pumping groundwater or water from high-capacity ponds sized for extreme earthquake conditions ('hardened safety core earthquake', defined in Chapter 36). This pumping system is independent of the emergency makeup that could be provided by using the facility's fire protection system.

In the first case, uncovery of the stored fuel assemblies could be the consequence of a loss of structural integrity of the storage compartment – or siphoning of the compartment – that could not be compensated by the water makeup systems. In order to exclude this type of situation, which would have very serious consequences, EDF has undertaken to check the structural strength of pool compartments.

In the second case, partial draining could lead to major effects such as degradation of the radiological ambient conditions in the fuel building or the reactor building, uncovery of a fuel assembly assumed to be blocked in the raised handling position, and significant boiling of the remaining water in the lower part of the storage compartment or in the reactor vessel.

Consequently, EDF decided to[509] install a system for automatic isolation of the FPCPS intake line, meeting the requirements applicable to the hardened safety core, and a system for automatic isolation of the drain valves on the reactor pool compartments, which must normally remain open during fuel handling. In addition, the ASN asked EDF to study modifications to components or operating conditions that would prevent fuel assembly uncovery during handling or a rapid drop in the water level above the stored fuel assemblies, which would result from a break in the transfer tube between the reactor building pool and the fuel building pool. EDF adopted the double-wall solution, which it intends to implement only in reactors for which it cannot demonstrate transfer tube resistance under extreme earthquake conditions.

IRSN also studied the possibility of a criticality accident resulting from water boiling in a spent fuel pool, leading to vaporization in the fuel storage area. The impact of a criticality accident of this type could explain certain phenomena observed or assumed during the Fukushima Daiichi accident:

- the large clouds of steam released above Unit 4;
- the high irradiation levels recorded near Unit 4 or in the reactor building on 15 and 16 March 2011;
- the rapid drop in the pool water level between 15 March and 16 March (see Figure 15.8), which would have caused the loss of leaktightness at the gate separating the reactor compartment from the spent fuel pool (Figure 15.9), then the relative stabilization of the situation until implementation of significant water makeup as of 20 March;
- increased hydrogen production by radiolysis, the possible source of the explosion in Unit 4.

Depending on how the storage racks are designed, a critical situation cannot be excluded in the event of water evaporation in the cells. Nevertheless, boiling and hydrogen production can only be significant if the critical state is maintained continuously or cyclically for several minutes. That does not appear very probable, given the instability of the parameters governing the nuclear reaction.

[509] As part of Phase 3 of the post-Fukushima modifications (see Chapter 36).

The explanation supported by TEPCO for the explosion of the Unit 4 building is that hydrogen was transferred when depressurizing the Unit 3 containment through the venting line to the stack common to Unit 3 and Unit 4[510].

Nevertheless, IRSN continues to conduct tests and develop simulation software to obtain a better understanding of the physical phenomena that could occur during an accident affecting a spent fuel pool, before and after uncovery of stored assemblies. Restoring operation of a cooling system also needs to be studied, as the cold water injected into a pool may transiently alter the established convection loops and lead to local overheating. A programme of studies and research (DENOPI) has been defined, based partly on work already undertaken in the context of international cooperation programmes.

15.5. Measures adopted for the EPR

The document entitled Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors (see Chapter 17), addressed to EDF in 2004, includes the following requirements relating to the storage of irradiated (spent) fuel:

– total loss of the pool cooling system must be studied for operating conditions with multiple failures (Risk Reduction Category A (RRC-A) – see Chapter 13). The designer must incorporate measures used to control this type of situation while maintaining the confinement function; otherwise, the probability of spent fuel pool water boiling must be reduced by making the appropriate improvements, in particular in the support systems for the pool cooling system;

– if the spent fuel pool is not located within the containment, 'practical elimination' of spent fuel melt situations in the pool must be demonstrated. This demonstration must include response to earthquake conditions.

The design option of storing spent fuel in a building separate from the reactor building was renewed for the EPR. As is the case for previous nuclear power reactors, the EPR fuel building features dynamic containment, without an obligation to maintain leaktight conditions: in the event of an accident leading to an abnormal rise in the pool water temperature, an outlet (rupture disc) must open to the outside environment. However, the fuel building has been placed inside a shell capable of withstanding an aeroplane crash.

The approach adopted by the EPR designers with regard to fuel-melt accidents in the fuel building aims to 'practically eliminate' situations where one or more fuel assemblies may be uncovered.

[510] The explanation supported by TEPCO is, however, debatable. Contamination was very low on the casings of the filters in the Unit 4 ventilation line that would necessarily have carried the venting gases from Unit 3: the dose rates measured on 25 August were less than 7 mSv/h, whereas dose rates higher than 10,000 mSv/h were recorded on 1 and 2 August 2011 near a containment venting pipe on Unit 1.

The Flamanville 3 EPR design has consequently benefited from improvements resulting from the new safety approach applied to spent fuel pools.

The pool cooling system used in normal operation has two completely independent and physically separate trains. Each train has two pumps, with emergency power supplied by the same electrical safeguard division, and a heat exchanger. In the event of total loss of heat sink, an emergency cooling system, cooled by a diversified heat sink (seawater pumped through a pipeline discharging 600 m from the pumping station), keeps the pool water temperature below 95°C.

Accidents potentially leading to spent fuel pool draining were taken into account in the design, in compliance with rules on design-basis accident operating conditions (see Plant Condition Categories in Section 8.1). It should be noted that the pool cooling system used in normal operation and the emergency cooling system are totally independent of the other fluid systems, so that a line-up error in these cooling systems cannot result in pool draining.

The layout adopted for the pipes connected to the spent fuel storage compartment is such that, in the event of a break, draining would stop before a fuel assembly being handled was uncovered, without intervention of an active isolation system. For some pipes connected to the lower parts of the compartments adjacent to the fuel storage compartment (transfer tube and drain pipes), the demonstration that no fuel assembly is uncovered in the event of a break is based either on automatic isolation devices, or on high-level design, manufacturing and operating requirements that aim to render a break in certain pipe sections highly improbable, with a high degree of confidence. However, the design is still subject to change; EDF is considering adding either plugs, or filters with a calibrated head loss, on the orifices of the pool compartment drain lines, which would be fitted in any state of risk (when lines are open between these compartments and the fuel storage compartment). These measures would make it possible to mitigate a guillotine break in these lines, in compliance with the design rules for design-basis accidents.

An emergency water makeup system (flow rate 150 m^3/h) and an ultimate emergency makeup system (flow rate greater than 35 m^3/h) would be provided to compensate for pool water evaporation and certain leaks (commensurate with the flow rate in the water makeup systems). These systems, combined with opening an outlet in the pool hall wall to the outside environment, would stabilize the water level in the spent fuel pool and remove any decay heat from the stored fuel assemblies through vaporization. Eventually it must become possible to start operation of a cooling system in order to allow the facility to reach and maintain a safe state.

15.6. Recommendations for new reactor designs

More recently, in ASN Guide No. 22 pertaining to the design of pressurized water reactors (already cited in previous chapters), a certain number of recommendations have been formulated on fuel storage safety. The guide's recommendations on underwater storage are discussed below.

▶ Events to be considered and general safety objectives

For spent fuel pool design and the associated safety demonstration, ASN Guide No. 22 recommends studying single initiating events that could lead to loss of pool cooling or a decrease in the amount of water in a compartment containing one or more fuel assemblies.

For the reference (design-basis) operating conditions of categories 2 to 4 (based on single initiating events):

- the measures taken to control nuclear chain reactions must ensure that the spent fuel pool does not reach criticality;
- a controlled state[511] must be reached, followed by a sustained safe state[512];
- cooling and confinement of the fuel stored or handled in the pool must be controlled; in particular, the fuel assemblies must stay under water and any radioactive release is to be filtered.

For situations covered by design extension conditions and more specifically by DEC-A (situations not leading to fuel melt, characterized by multiple failures), appropriate attention should be given to plausible situations of:

- long-term loss of off-site and on-site power (power supplies required to maintain control of reference operating conditions);
- long-term loss of any systems required to remove decay heat to the heat sink under reference operating conditions;
- total loss of the spent fuel pool cooling system;
- a reference operating condition combined with failure of the measures intended to ensure its mitigation.

The objectives of the DEC-A conditions are as follows:

- reactivity must be kept under control; subcriticality in particular must be maintained over the long term;
- decay heat removal from the spent fuel pool by boiling may be acceptable temporarily if a sufficient water level is maintained in the pool;
- radioactive substances are confined; for this purpose, the design aims to avoid radioactive release to the environment;

[511] Subcriticality, decay heat removal and confinement of radioactive substances are ensured in the short term. The spent fuel pool water inventory is stabilized or increasing, and no assemblies are uncovered.

[512] Subcriticality, decay heat removal and confinement of radioactive substances are ensured in the long term. No assemblies are uncovered in the spent fuel pool, and stored fuel decay heat removal by the main heat sink has priority.

– the facility must be capable of autonomous operation within a time frame compatible with the response time for intervention by off-site services, in particular with regard to facility electrical power supplies and the heat sink, in order to be able to manage the reference and design extension operating conditions, including long-term conditions affecting both reactors and spent fuel pools. Good practice would be at least 72 h of autonomous operation.

The radiological consequences of the accidents covered by reference operating conditions and DEC-A conditions, without fuel melt, must be as low as reasonably practicable and, in any case, must not lead to the need to implement population protection measures (no sheltering, no stable iodine administration, no evacuation).

The design recommendations defined below eliminate the need to take into account situations with fuel melt (DEC-B) in spent fuel pools.

▶ Design recommendations

In ASN Guide No. 22, it is emphasized that fuel assemblies must be designed to maintain their integrity in storage, transport and handling situations before and after irradiation in a reactor. Although fuel must be designed to avoid any loss of leaktightness in the reactor under normal and incident operating conditions, the potential presence of a few cladding defects in normal operation must be taken into account in the safety demonstration, as well as fuel-related operations after irradiation in the reactor.

Fuel assembly storage must be designed to ensure that no criticality situation, within specified margins, arises in normal storage conditions or in incident or accident situations. It must also be designed to ensure that there is no uncovery of spent fuel assemblies while they are stored under water or during handling.

Fuel assembly storage must be designed to ensure that the irradiation level in the building is compatible with the activities of workers and outside contractors defined in the normal storage conditions or in incident or accident situations.

In reference operating conditions, when a reference hazard occurs, and in DEC-A conditions involving the loss of only the main pool cooling system, the facility design must allow the operator to maintain the pool water temperature below boiling within a sufficient margin given the estimated frequency of the event considered.

In the event of total loss of the pool water cooling systems (DEC-A condition), one or more other systems must be capable of:

– averting fuel assembly uncovery by sufficiently compensating for water loss by boiling,

– maintaining a water level in the pool that is sufficient for restarting a cooling system.

Implementation and operation of a spent fuel pool cooling system must be possible after a prolonged loss of cooling that resulted in boiling, and must allow the facility to reach and maintain a safe state.

The spent fuel pool must be equipped for leak detection and collection.

The design must ensure that no leak or break in a system connected to the spent fuel pool leads to uncovery of the fuel assemblies stored or being handled. The lower part of the compartment(s) accommodating the fuel assembly storage racks must not be connected to any system lines; must not be subject to siphoning; and must not be subject to uncovery due to loss of water in an adjacent compartment, under any circumstances whatsoever.

Structural components of the storage compartments must be designed with large margins that are commensurate with the loads likely to be encountered (earthquake conditions, a falling load, thermal stresses due to boiling, etc.). Structural components must be sufficiently resistant to allow the storage compartment to fulfil its safety functions in the event of a design extension condition earthquake.

In general, safety functions must avert fuel melting in the spent fuel pool in the event of any naturally occurring hazards covered in the design extension conditions.

15.7. New systems for storing spent fuel

Looking beyond the improvements already implemented by EDF, reinforcing safety of underwater spent fuel storage and handling in the spent fuel pools of reactors in operation, up to and including the N4 series, is one of the objectives of discussions pertaining to the extension of their operating lifetime. The aim is to converge with the requirements defined for the EPR, as far as reasonably practicable. In this regard, two modifications planned in the context of the fourth ten-yearly outage of 900 MWe units described earlier aim to provide functional redundancy of the isolation of the FPCPS intake line and a backup for the system (‘FPCPS 2’).

Moreover, the spent fuel storage capacity available in the pools of operating reactors and in the Orano facility at La Hague appears to be insufficient[513] (particularly if the operating lifetime of the reactors in service is extended beyond 40 years). For this reason, in June 2013 ASN asked EDF to “revise its strategy with regard to spent fuel management and storage[514], by proposing new storage systems to cover the needs and to reinforce the safety of fuel storage.”

EDF has planned to build[515] a ‘central storage pool’ mainly for storing fuel assemblies from the pressurized water reactors of nuclear power plants[516], which could feature several units (or pools).

[513] Observation shared by EDF and Areva, for example at Advisory Committee meetings on the fuel cycle (in 2001 and 2010), where it was observed that the La Hague pools could be full by 2030.

[514] This strategy was based on a project to increase storage density in the spent fuel pools of the CPY series 900 MWe units. After review by IRSN, this strategy was not judged satisfactory by ASN.

[515] On a site not yet defined at the date of publication of this book.

[516] As well as those of the SUPERPHENIX reactor (at the Creys-Malville nuclear power plant), currently stored on site in the Spent Fuel Removal Unit.

In July 2019, following the technical review led by IRSN and a meeting of the Advisory Committee for Nuclear Laboratories and Plants, the ASN informed EDF of its opinion[517] on the safety options report for the central storage pool, submitted by EDF in April 2017. In the letter of notice of ASN's opinion, an important point concerns the risk of accidental draining of the central pool following a break. With regard to this point, EDF planned to conduct a study to demonstrate that the configuration of the area under the pool, where seismic bearing pads are located, would avoid fuel assembly uncovery if the pool were to be drained suddenly. ASN defined the objectives to be met to support this argument, considering it is "necessary that [in the central pool construction authorization application] EDF define passive measures for keeping stored or handled assemblies under water in the storage pool and in the transfer canal, for a postulated scenario of massive accidental draining of a storage pool or a transfer canal in the facility following a break in a structure ensuring their integrity, within a time-frame that is compatible with the time required to implement the mitigation equipment and procedure for this situation."

[517] This opinion was sent by ASN in a letter dated 29 July 2019, reference CODEP-DRC-2019-033736.

Chapter 16

Taking into Account Human and Organizational Factors in Facility Design

The major importance of organizations and human actions in ensuring the safety of facilities such as nuclear power reactors was highlighted in Chapter 4 of this book, where the concept of human and organizational factors (HOFs) was first explained.

The purpose of this chapter is to discuss how these factors are taken into account in the initial design phase of nuclear power reactors and during the design of modifications that are made during their operation (excluding dismantling).

16.1. Taking into account human and organizational factors in nuclear power reactor design

16.1.1. Importance of considering human and organizational factors at the design stage

▶ Historical perspective

When the French programme to build nuclear power plants with pressurized water reactors was launched in the 1970s, the nuclear safety of these facilities was mainly discussed in terms of technical reliability. The designers also aimed to reduce the possibility of human error by automating certain actions and structuring the activity of operating crews through various rules and procedures. Implicitly, what was expected of these teams was that they operate the technical systems by faithfully applying the operating (and maintenance) procedures that aimed to 'contain' the operation of the system within safe limits. These procedures were supposed to make it possible to deal with all situations the designers had planned for.

During the accident at the Three Mile Island (TMI) nuclear power plant in March 1979 in the USA, things did not go as planned. The shift personnel, based on indications in the control room, made an incorrect diagnosis due to a human-machine interface fault. This contributed to transforming an ordinary event into a core-melt accident.

#FOCUS

What happened during the accident at Three Mile Island[518]?

A pressurizer relief valve, which had opened automatically to limit the pressure peak in the reactor coolant system resulting from secondary system incidents, did not return to its closed position, even though the reclose command had been issued by the instrumentation and control system. The control room interface used the reclose command to the valve as information instead of its real position (blocked in semi-open position), which gave the operating crew an inaccurate view of the state of the facility. In addition, the reactor trip (automatic emergency shutdown) and problems affecting the secondary system set off multiple alarms. In the absence of a hierarchical display of information, the crews were overwhelmed, struggling to see and extract the relevant information, their task made more difficult by the fact that some of the indications (such as the valve position) were inaccurate. The operators stopped automatic safety injection due to this inaccurate information and because they followed the instruction to maintain the steam bubble in the upper part of the pressurizer.

The lessons learned from the TMI accident (and others) seriously called into question the model[519] of human intervention in nuclear power plant safety. Gradually,

[518] This accident is described in greater detail in Chapter 32. The discussion in this chapter only covers those aspects relevant to human and organizational factors.

[519] The term 'model' is used here with the meaning it has in the social sciences, i.e. a schematic representation describing and illustrating the main characteristics of an object, system, or process in a reductive, simplified and functional manner.

the event analysis[520] went beyond the operator error analysis and focused more broadly on the failures of the overall sociotechnical system that led to these errors, failures, or the combination of both. One of the lessons learned from the TMI accident was that control room design plays a determining role in the control of incidents and accidents in terms of prevention as well as mitigation of consequences for situations occurring despite the preventive measures taken. Procedures and the organization of operating crews also play an important role.

With this accident, human and organizational dimensions became part of the scope of controlling risks at the design stage and during operation of nuclear power plants.

The lessons learned are not specific to the nuclear field. In the 1980s, many studies focused on operator activities in 'control centres' or control rooms of 'continuous processes' (such as refineries, cement plants and steel mills). They brought to light the complexity of the monitoring function performed in the control room and highlighted the role of 'anticipation' by the operators carrying out this function. Their aim is to predict the physicochemical changes in the 'processes' that they monitor. They may thus act before an alarm or fault appears in the control room (in other words, they "do not operate according to the alarms").

The operating safety of an industrial facility potentially exposed to risk comes into play from the design stage. The TMI accident led to significant changes in recognizing the importance of organizations and human action in the safety of nuclear power plants.

In France, starting in the 1980s, this heightened awareness led Électricité de France (EDF) to make the N4 series (1450 MWe reactors) innovative both in terms of control room technology, compared to earlier series, and in terms of considering human and organizational factors at the design stage[521]. In 1982, after analysing several technical solutions, EDF also decided to design an entirely computerized control room (see Figure 16.1). This was a major innovation because no control room of this type had ever been installed anywhere in the world for a nuclear power plant[522]. Furthermore, EDF decided to develop a control room simulator[523] as part of this approach. This simulator, named S3C, contributed to the design of the computerized instrumentation and control system and to incorporating human and organizational factors throughout the design of this control room. The simulator also helped EDF implement a significant

[520] Readers may wish to refer to *L'accident de la centrale nucléaire de Three Mile Island* (The Accident at the Three Mile Island Nuclear Power Plant) by M. Llory, L'Harmattan, 1999.

[521] *Palier N4 : apports de l'ergonomie dans la conception de la salle de commande* (The N4 Series: the Benefits of Ergonomics in Designing the Control Room), B. Le Guilcher and Y. Dien, *Revue générale nucléaire*, no. 1, pp 27-32, January-February 1998.

[522] *Palier N4 : examen du rapport provisoire de sûreté* (The N4 Series: Preliminary Safety Report Review), L. Samier and J.-M. Mattéi. *Revue générale nucléaire*, No. 4, pp 11-14, July-August 1996.

[523] This was not yet a complete or 'full-scale' simulator of a control room for the N4 series reactors. The S3C simulator was installed in the training centre of the Bugey nuclear power plant. In general, in this type of simulator, CATHARE simulation software, presented in Chapter 40, is used to represent changes in the 'process'.

programme of successive ergonomic evaluations to validate equipment such as the operator workstations in the control room[524].

Since changes in the N4 series control room from the HOF perspective have been used as an example to illustrate certain points discussed in this chapter, the following focus provides further details on this control room.

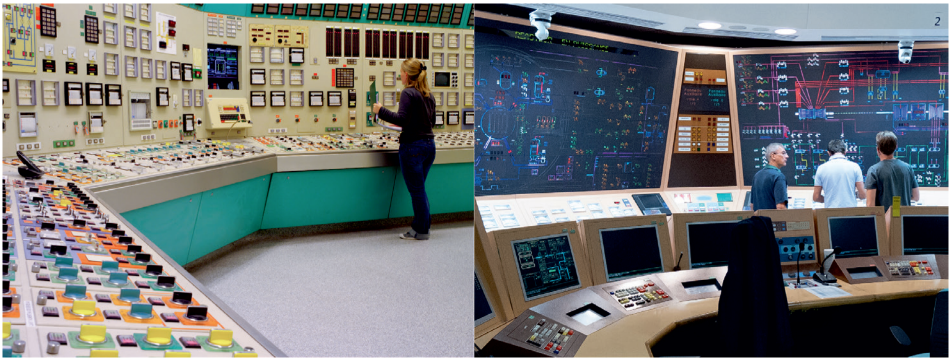


Figure 16.1. Left: conventional control room (Fessenheim nuclear power plant) EDF Media Library – Mario Fourmy. Right: computerized control room of an N4 series reactor (Civaux nuclear power plant). Romain Beaumont, photographs.

#FOCUS

Control room of N4 series reactors[525]

Four workstations were used for the control room of the N4 series reactors. They are identical, provide access to the same database, and thus make mutual assistance possible. They can be locked into an observation-only mode using a key (inhibiting any action on the ‘process’). Two of them are control workstations for control operators, whereas the two others are observation and monitoring workstations for the shift supervisor[526], shift manager or safety engineer.

A plant overview panel shows the main facility parameters, the state of the main actuators and the state of safety systems. These components can be seen at the operator workstations. This plant overview panel makes it possible to:

[524] *Palier N4 : apports de l’ergonomie dans la conception de la salle de commande*, ibid.

[525] These summarized descriptions are excerpts taken from the document *La salle de commande du palier N4 : principales caractéristiques et retour d’expérience d’exploitation* (The N4 Series Control Room: Main Characteristics and Operating Experience Feedback), J.-M. Peyrouton, J. Guillas, and C. Nougaret, EDF-DPN.

[526] Later called the ‘deputy shift manager’.

– give operators a rapid, overall view of the state of the facility and correct the incomplete view provided by the display screens,

– provide a common reference as to the state of the facility to the various members of the operating crew, helping to coordinate their actions as a common analysis tool.

Diversified control systems are found in the control room, in the form of an auxiliary panel, equipped with conventional control systems, that is independent of the computerized control system (KIC) to which the operator workstations are connected. From this auxiliary panel, it is possible to bring the reactor to a safe state and control incident and accident situations. This auxiliary panel is only used when the computer system is unavailable (due to a failure or scheduled outage).

There is also a remote shutdown station, outside the control room and at another level in the building, which, in case of fire in the control room, allows the operators to bring the reactor to a safe state. To be consistent with the control room, the remote shutdown station has the same operator interface as the auxiliary panel.

Compared to earlier series, the following provisions were not called into question during the design process:

– composition and organization of the operating crew,

– level of automation, which remains similar to that of 1300 MWe reactors.

About 800 control displays may be accessed by operators (displays for control, monitoring settings, etc.), along with more than 4000 alarm sheets and about 10,000 technical sheets (for the various actuators, measurement sensors) which provide information in real time. There are about 2000 'procedure displays' for normal operation and 2000 'procedure displays' for operation according to the state-oriented approach (SOA – see Chapter 33).

Computerized operating procedures are interactive flowcharts showing the basic operator actions. Each operator action or decision called for as a step in the flowchart is checked by the computerized control system KIC, which ensures consistency between the operator's choices and the data he or she has from the system. By using this type of procedure, operators are guided in their choices and actions. They can, however, 'override' a procedural instruction if necessary, for example if they have information the system cannot acquire.

▶ Current situation

Incorporating human and organizational factors (HOFs) in the design of nuclear reactors has today become systematic and the related objectives are explicitly stated in nuclear safety regulations. In the French Order of 7 February 2012 setting the general rules for basic nuclear installations ('INB Order'), the operator is asked to implement an approach that, from the design stage, "takes into account all relevant technical aspects, organizational factors and human factors".

In addition, there is now abundant technical documentation and scientific literature in the form of guides, standards, books, articles and reports, at both the national and international level, to support designers in designing a nuclear power plant with an integrated approach including technical, organizational and human aspects (some of these references will be cited in this chapter).

In France, experience acquired, mainly during the design and safety assessment of the N4 series reactors, then the EPR, has led the French Nuclear Safety Authority (ASN) and IRSN to jointly prepare a document[527] of recommendations on the design of new nuclear power reactors. This document indicates that a nuclear power plant "is a sociotechnical system whose operation is based on the interactions between workers, an organization, technical equipment and a physical work environment. The sociotechnical system must be designed to create the most favourable conditions possible for the personnel to conduct the activities related to facility operation, in normal conditions as well as in the case of incident, accident or hazard conditions (as defined in the design basis and design extension conditions)."

▶ Operating experience feedback: some inappropriate design choices

Avoiding situations where operators might make mistakes must therefore be an important priority from the design stage of a nuclear power plant. Analysis of the operating experience feedback (OPEX) from nuclear power plants in operation shows that certain design choices inappropriate to reality in the field have led to operator errors and significant events (this concept is detailed in Section 21.4). For example, faults in computerized control displays and operating documents contributed to a monitoring failure in 2010 in the control room of Unit 1 at the Civaux nuclear power plant. The monitoring failure concerned the fire protection system for the auxiliary transformers. It remained in an inappropriate configuration for a month before this anomaly was detected. Another example dates from 2009, when an information display system screen in the control room (not computerized) at Fessenheim 1 was only displaying five parameters, whereas the operating document called for operators to monitor 14 sensors in real time. This contributed to the delayed detection of an exceeded threshold. Similarly, in 2011, the absence of an alarm and an alarm window lighting fault in the control room of Paluel 1 resulted in the non-detection of a coupling fault between a diesel generator and a switchboard. Also in 2011, it was discovered that information on emergency equipment for Unit 4 at the Bugey nuclear power plant (the emergency feedwater system turbine-driven pump and the emergency turbine generator) could only be consulted locally, in a controlled area. Due to the time necessary to change clothing before entering this area, this design choice obliged the plant operator to set up a specific organization during the operating phases of this equipment, which involved mobilizing duly equipped field operators.

[527] ASN Guide No. 22: *Conception des réacteurs à eau sous pression* (Pressurized Water Reactor Design), 18 July 2017.

Significant events resulting from design choices may cause problems not just for operations in the control room. For example, in 2004 at Belleville 2, the control device on a valve was in the low position and was operated incorrectly by a field operator[528], leaving the valve open instead of closed, subsequently reducing the water level in the fuel storage pool.

While these few examples did not have serious consequences because of other 'lines of defence', from the design stage to avoid placing operators in situations that could lead them to make errors or in which it would be difficult to return to a normal situation – one of the objectives of safety being to avoid the occurrence of incidents as much as possible.

16.1.2. Approach at the design stage

As indicated above, design does not only involve designing technical systems or devices. It plays a significant role in creating 'work situations'[529] in which operators carry out activities to operate the facility. However, in real operation, these situations are highly variable. Contingencies occur, and organizations and workers have to adapt, sometimes to the detriment of performance, nuclear safety, or even their own health and personal safety.

Nuclear safety thus assumes that the technical, human, and organizational components of the sociotechnical system are interlinked; but how are they to be incorporated in design?

[528] Usually valves are installed on systems with the control device set to the high position. The wheel is then turned clockwise to close the valve, which is standard use. When the control device is set to the low position, the wheel must be turned anticlockwise to close the valve. Even if operators know there are valves where the operating direction is reversed, they may still become confused and operate these valves in the usual direction, especially when other factors such as time pressure, stress, interruptions, etc. disrupt their activity.

[529] In ergonomics, the work situation is defined as the "concrete context where workers engage in material or immaterial production, in a given set of working and safety conditions" (Rabardel *et al.*, *Ergonomie, concepts et méthodes* [Ergonomics, Concepts and Methods], Éditions Octarès, 1998). In this same book, the working situation is described as a system made up of many elements that determine and influence the real work of operators: the technical systems and equipment, work organization, the workers and their skills. This definition gives the context a broad meaning that is determinant in the operator's understanding of work situations. Daniellou and colleagues define components of a work situation, some of which are visible to operators (facility, tools, co-workers, etc.) while others are more invisible (company strategy, facility and operator history, labour relations, organization rules, management style, etc.) (in *Les facteurs humains et organisationnels de la sécurité industrielle : un état de l'art* [Human and Organizational Factors in Industrial Safety: the State of the Art], *Les Cahiers de la sécurité industrielle 2010-02, Fondation pour une culture de sécurité industrielle*, 2010). Other authors speak of remote determinants, inaccessible to operators, that "implicitly influence the situation" (Journé & Raulet-Croset, *La décision comme activité managériale située – Une approche pragmatiste* [The Decision as a Situated Managerial Activity – a Pragmatic Approach], *Revue française de gestion – Éditions Lavoisier* – 2012/6 No. 225, 109-128, available at https://www.cairn.info/revue-francaise-de-gestion-2012-6.html).

A first key step is analysing 'existing elements' (experience feedback from design projects, events or other forms of knowledge). This analysis provides indispensable data for determining the needs related to the operating activities (in terms of equipment, documentation, as well as organization), defining the corresponding design requirements and conceiving appropriate technical and organizational provisions. A second essential step is validating the implemented provisions before the facility is commissioned. Thus, in compliance with recommendations in the ASN Guide cited above concerning the design of pressurized water reactors, "design provisions must be identified progressively and, if necessary, iteratively, in three phases: analyses to define design requirements, definition of provisions, and validation that the planned provisions adequately fulfil the formulated requirements".

Experience shows that during commissioning and afterwards, it is important to evaluate, in the workplace, the ability of teams to perform the activities required for facility operation in order to make any necessary adjustments.

16.1.2.1. Prior to the design phase: analysis of 'existing elements'

It may seem paradoxical to analyse work situations that do not yet exist from the start of the design phase. Nonetheless, this is a key step on which the facility's design depends. Analysing real work situations in operating facilities makes it possible to identify elements or factors that have the likelihood to influence operator activities and that have not yet been taken into account in the design. For example, in the control room, in certain situations the control operators may need information from a temperature sensor to be able to react quickly instead of waiting for a field operator working locally to provide the value from the sensor. If this need is not correctly identified at the design stage[530], a detected state may be delayed in reaching the control room, thereby delaying corrective action.

[530] During commissioning tests or later, during reactor operation, before such situations occur, in which case a modification can be made to the facility. Scenarios that are 'played out' on control simulators are limited in number, and they do not reproduce all of the variety and complexity of real operating conditions (interactions between operation and maintenance, disturbances and other situations the operating crews are confronted with). A real event in May 1998 in Unit 1 of the Civaux nuclear power plant illustrates this point. A break occurred in the residual heat removal system (RHRS) inside the containment. The reactor's initial startup tests were underway. Incident operation, according to the 'state-oriented approach' (SOA), began on 12 May, with the return to a stabilized state not occurring until 12 June. The triggering of fire detection alarms, concomitant with the break, complicated the early management of the event and led to an inappropriate operating strategy. Leaking steam had in fact set off the alarms (the break was in the connection between the RHRS system and the chemical and volume control system). The combination of a thermal-hydraulic event with a fire had not been anticipated when the computerized control system was developed. In addition, the shift personnel had difficulty applying the operating procedure for breaks occurring in the 'reactor coolant system closed with the RHRS connected' configuration. For more than nine hours, the operators continuously 'looped' through this procedure without locating or isolating the leak. It was only through the national emergency response and by taking actions that bypassed procedures that the event was finally brought to an end. Its analysis identified a very large number of steps that were overridden by the operators in applying the operating procedures recommended by the computerized system.

It is essential for analysis of real work situations to consider characteristic operating situations (also called 'reference situations') in the various areas important to risk control, such as control activities and maintenance. For example, in the control room these situations include the approach to criticality, reactor startup, process monitoring and periodic testing, or, in other rooms, maintenance operations and fuel assembly handling, etc. The corresponding analyses serve to characterize the diversity and variability of contexts in which the operators work (shutdown states, operating transients, etc.), to identify interfaces between different disciplines and to determine what, in real work situations, may facilitate operator activities or, on the contrary, make them more difficult.

But, more broadly, analysis is also based on three other types of information:

- experience feedback from previous design projects, so that weak and strong points can be identified,
- experience feedback from events,
- knowledge from studies as well as research and development.

In these three areas, information is to be sought not only nationally but also internationally.

The analysis term 'existing elements'[531] covers all of the areas mentioned above.

▶ Example of the N4 series

The N4 series example is developed here to illustrate this chapter's point. Human and organizational factors were taken into account in the design of this series (in the second half of the 1980s and beginning of the 1990s) by using the lessons learned during the design, construction, and early operation of the previous nuclear power reactors in France, and using international experience feedback. But while EDF made considerable efforts in control room design with regard to incident and accident operation management, with test campaigns on the S3C simulator starting in 1986 for the purposes of ergonomic evaluations, it became clear that the design of control systems and resources for normal situations was not based on sufficient observation of activities in real work situations prior to the design phase (analysis of 'existing elements').

This is why in 1995, following the safety assessment of the instrumentation and control system of the Chooz B1 reactor (the first N4 series reactor to be commissioned in 1996), the Directorate for the Safety of Nuclear Installations considered that it was necessary for EDF to evaluate how this reactor control room was used from an ergonomic point of view during its first operating cycle. The evaluations conducted by EDF in 1998 and 1999 brought to light several difficulties for operators during normal operation, involving monitoring activities (lack of an overview of the reactor state and its changes, structure of the control displays, etc.) as well as more general control room activities. These difficulties included the unsuitability or lack of dedicated tools

[531] Expression adopted in the HOF field.

for performing certain activities such as taking readings at the start of the shift or conducting periodic tests.

The ‘ergonomic assessment reports’ submitted by EDF showed that the difficulties were not related to computerization of the control room, but rather to inadequate consideration of human and organizational factors in the design process. Because there was a lack of analysis of operator activities in ‘reference situations’, the designers were unable to determine the appropriate requirements before designing the actual systems to be implemented, such as the displays providing operators with an overview of the state of the facility and the control systems and resources for conducting periodic tests. As a result, a periodic test performed in ten minutes for the 1300 MWe units required referring to 54 displays and completing three hours of work to obtain the corresponding values for the N4 series units.

These observations led the Directorate for the Safety of Nuclear Installations to ask EDF to “improve the computerized interface of the N4 series unit for normal operation.” The programme of action was to include “a presentation of the improvements planned with the main associated requirements (tasks and design elements, access to information, error handling, etc.) and objectives to be met in terms of expected performance of the operating crew (task performance time, detection times, etc.).”

EDF thus set up a significant programme of changes to the computerized control system in the N4 series. These changes led to modifications in the computerized control system (KIC). EDF proceeded with the development and implementation of ‘computer-aided control displays’ to improve operation in normal situations. To design and validate these changes, EDF adopted an approach explicitly taking into account human and organizational factors at various stages of the modifications, including observations made using the simulator. Implementing this approach was an improvement. It involved explicitly taking into account human and organizational factors at the various stages of the changes[532].

To design the EPR, EDF drew on lessons learned from the difficulties encountered during the design and startup of the N4 series units and analysed real situations and experience feedback from the detailed design phase of the project. Analyses of activities in real operating situations of reactors already in operation were conducted, based on ergonomic studies for 1300 MWe and 1450 MWe reactors. The data collected from interviews and observations made it possible to identify typical activities and determine the requirements in terms of necessary information, means of action, etc. In addition to this operating experience feedback for incident and accident operating situations, an analysis was made of significant event reports.

[532] This approach was consistent with the recommendations in documents such as international ISO standards and guides published by the U.S. NRC in the USA.

16.1.2.2. Design objectives

The results of the 'existing elements' analysis make it possible for the designers to define, from the beginning of the design phase, the main objectives in terms of taking into account HOFs. These objectives are important because they guide certain choices for technical and organizational provisions and their implementation.

For example, to design the control room of N4 series reactors, EDF set two main objectives:

- provide operators with access to information and control systems and resources they will or may need at the appropriate time, rather than permanently displaying them in the control room,
- provide operators with a limited amount of reliable and representative information at a given time.

These objectives led EDF to assign computer systems of the N4 series reactors a much more important role than for the 1300 MWe reactors, which were already equipped with various types of computer equipment for facility operation. After making the choice to computerize the control room of N4 series reactors, EDF used various design orientations for operation of these reactors: desired level of control automation, composition of the operating crew and roles in the various anticipated situations (normal, incident or accident), principles of certain forms of computer-aided control such as alarm sheets, procedures, etc.

These orientations then guided the detailed design of the control room. For example, the designers decided that any computer workstation for operating crew members in the control room would feature the control systems required for both normal situations and incident and accident situations. They also decided to provide (and thus develop) computer-aided control resources (computerized procedures, etc.).

As for IPSN, in 1984, as part of its assessment of the preliminary safety analysis report of N4 series reactors submitted by EDF, it evaluated the design objectives and orientations by drawing on general knowledge concerning operators' activity in the control room and on studies concerning the operation of pressurized water reactors in accident situations. These studies were conducted in 1982 on the 'full-scale' CP1 simulator of the Bugey nuclear power plant as part of a four-party agreement (between IPSN, EDF, Framatome and Westinghouse) regarding lessons learned from the accident at the TMI nuclear power plant.

IPSN examined the consequences of computerizing control systems in the control room and identified some associated subjects and questions. For example, one of the subjects concerned the mechanisms of collecting and processing information in incident and accident situations. Based on general observations (for the control of various industrial processes), operators feel the need, in a disturbed situation, to verify the corresponding information and perform multiple readings to make sure they did not make an error. One of the questions was how, on computer screens, operators could make sure they did not make an error in reading the information (checking the information, multiple readings, etc.).

IPSN also raised questions on responding to alarms and the importance of the control room for performing maintenance activities and periodic tests. Another question was how the operating crews would manage computer system failures and how these failures would influence operators' activities.

In the 2000s[533], concerning the design of control systems for the EPR, EDF presented the Directorate General for Nuclear Safety and Radiation Protection with its instrumentation and control objectives in the form of 'essential choices' concerning the corresponding systems and the respective roles of workers and these systems. These essential choices were based notably on operating experience feedback from the N4 series: use of computerized operating procedures, level of control exercised by instrumentation and control on the actions performed by the operating crews, and structure of the control displays. EDF also defined principles of organization for operating crews concerning the assignment of responsibilities, the workloads, and the 'line of defence' that consists of assigning control to the shift supervisor and assigning checking to the safety engineer.

16.1.2.3. Definition of detailed design provisions

The term 'design provisions' covers all technical and organizational measures that enable the relevant teams to operate a nuclear power plant.

Technical provisions cover an extremely broad area. This includes not only equipment such as control systems in the control room (computer workstations, plant overview panel, computerized control displays, control buttons, alarm windows, etc.), equipment in other areas (electrical switchboards, valves, pumps, measuring instruments, etc.), access issues (room layout, ladders, doors, electrical outlets, lighting, etc.), but also all the documentary resource used for operation (procedures, operating sequences, etc.).

Organizational arrangements involve the distribution of roles and responsibilities in the teams (for operation, maintenance, etc.), the definition of these teams and the necessary skills, interfaces between the various disciplines, meetings for coordination and exchange of information, etc.

Designers must therefore define detailed technical and organizational provisions that comply with the project's orientations and fulfil its objectives, while giving due consideration to the analysis and needs from the 'existing elements'.

[533] Incorporating human and organizational factors had already been addressed in discussions on the nuclear safety objectives and design options of the EPR.

▶ Operational needs

Concerning operational needs, experience feedback highlights the importance of the following points:

1. They concern all activities related to the operation of a nuclear power plant, i.e. all activities during which the teams interact with the facility.

2. They must take into account the analysis of 'existing elements'.

3. The operational needs to be defined for the design of a new reactor do not necessarily result directly from observations in existing power plants, since the technical characteristics of a new reactor may be different[534]. In this case, designers must identify needs for the new facility based on the technical characteristics known at this stage, making it possible for them to imagine future work situations and derive appropriate provisions.

   For example, observations of a facility's monitoring activity in a conventional control room[535] show that this activity is based on an initial appraisal of information at the start of each shift, which includes consulting various panels in the control room (called 'panel walkdown'). Information is displayed on geographically stable media and is continuously shown on panels and consoles, making it easy to locate information quickly. In addition to building this representation of the state of the reactor, information is exchanged when the shift personnel changes every eight hours ('shift turnover'). This initial representation changes throughout the shift by the more or less systematic monitoring of the various parts of the facility, according to information displayed on panels and consoles and exchanges in the control room.

   When EDF made the choice in its design orientations to computerize the control room of the N4 series reactors, the designers had to define design provisions that made it possible for operators to perform this monitoring activity, but using different systems. Computerization does not remove the operators' need to build and update an overall and shared representation of the state of the reactor they operate. Based on this need and the associated design requirements (see below), the designers' task was thus to define the monitoring activity as it might be performed in the computerized control room – this definition then had a strong influence on structuring the control displays on the computer workstation screens and on organizing the information presented in these displays.

4. Throughout design work, more targeted or detailed analyses of the 'existing elements' may turn out to be useful for obtaining more accurate data, depending on the project phase. For example, as long as the design of certain

[534] This may involve innovative reactors, as opposed to 'evolutionary' reactors.

[535] Control room in which the control systems and resources (information, control devices) are not computerized. They are displayed on panels on the walls of the room and on consoles (see Figure 16.1).

systems is not finished, it may be difficult to completely define the operational strategies and corresponding operator actions, and thus the information required by operators to take these actions.

▶ Design requirements and definition of appropriate provisions

The formulation of design requirements is based mostly on the analysis of existing activities and extrapolation to the activities to be performed in the new facility.

Continuing with the example of computerizing the control room of the N4 series reactors, operators' need to build a representation of the reactor state and to make changes to it over the course of the shift, no longer with a 'panel walkdown', but with control displays on a computer workstation, has led designers to adopt requirements concerning the control displays. Continuing with point 3 above, a general requirement is that the control displays should be structured to provide summary information easily accessible to the operators, enabling them to build a mental picture of the reactor state and follow any changes over the course of the shift. Another requirement concerned obtaining a representation shared by the members of the operating crew and the means of coordination between them.

As indicated above, for this purpose designers may also draw on standards, guides, and other information from the state of knowledge (including lessons learned from experience feedback).

ASN Guide No. 22, already cited, thus indicates that the control room "must be designed to provide appropriate and sufficient information to the operators for:

- obtaining a diagnostic on the facility state and on the efficiency of safety-related systems,
- checking the availability of technical and human resources needed to deal with the situation[536],
- assessing the effects of their actions."

These are very general recommendations. There are also currently available documents published nationally or internationally, containing more detailed recommendations. Among these are the following standards released since the 1980s (and updated):

- Standards published by the International Electrotechnical Commission (IEC), in particular standard IEC 60964 on control room design for power reactors. It is often used with standards on more specific aspects, for example IEC 61839 on functional analysis, IEC 61227 on information and control systems, IEC 61772 on display screens, etc.;
- standards published by the International Organization for Standardization (ISO), in particular ISO 9241 on the ergonomics of human-system interaction, ISO 11064 on the ergonomic design of control centres for industry and

[536] Normal operation, incidents and accidents, including those with core melt.

transport, and ISO 13407 on human-centred design processes for interactive systems (revised in 2010 as ISO 9241).

Detailed guides have also been produced by some countries, such as:

- NUREG-0700[537] published by the U.S. NRC;
- the guide MIL-STD 1472[538] published by the US Department of Defense (DoD). This guide contains particularly valuable information for designers. Other guides have been published by the DoD, such as MIL-HDBK-0759C[539];
- the guide[540] published in 2004 by the Electrical Power Research Institute (EPRI) in the USA, which deals with control room design, including modifications.

By contrast, there are few recommendations on defining organizational provisions. However, validation of provisions adopted in the design phase makes it possible to assess the provisions for organizing teams in charge of operation (control room teams, field operators, relations between 'disciplines', etc.).

16.1.2.4. Validation of design provisions

Beyond the elements discussed above involving the design approach, including human and organizational aspects, notably 'ergonomic assessments', it is essential to check and then validate that the provisions adopted and implemented meet the defined needs satisfactorily[541].

▶ General principles

To validate the ability of teams to operate the facility using the control systems and resources in the control room as it is designed, it is essential to perform integrated system tests on a full-scale simulator[542] before commissioning the facility. These tests must be performed in conditions as representative as possible of the situations that operators may encounter during operation. For the validation of the computerized control room of the N4 series, five test campaigns were performed from 1987 to 1996.

[537] Human-System Interface Design Review Guidelines – NUREG-0700, Revision 2, published in May 2002, U.S. NRC.

[538] DoD Design Criteria Standard: Human Engineering – MIL-STD-1472-G – January 2012. Department of Defense (USA).

[539] Handbook for Human Engineering Design Guidelines, MIL-HDBK-759C, July 1995. Department of Defense (USA).

[540] Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance, EPRI, Palo Alto, CA, the U.S. Department of Energy, Washington, DC: 2004. 1008122.

[541] Consistent with the design process called the 'V-model' in design engineering.

[542] As indicated earlier, the S3C simulator was installed at the training centre of the Bugey nuclear power plant. The N4 series full-scale simulator was installed at the training centre of the Chooz nuclear power plant. For the EPR, the full-scale simulator was installed at the training centre of the Flamanville nuclear power plant.

For the Flamanville 3 EPR, four campaigns were performed from 2009 to 2016. As part of startup tests, HOF observations have been planned from the outset.

The results of tests conducted during the validation phase must, of course, be considered as well-founded and reliable. Preparing and performing tests on a full-scale simulator requires that the following points – in addition, of course, to the simulator's representativeness – be carefully considered:

- organization and skills of the team in charge of validation,
- definition of scenarios to be tested based on operating situations,
- expected knowledge and skills of those participating in the tests,
- conditions for performing the tests and collecting the data,
- analysis and interpretation of the data collected.

Before these integrated system tests are conducted on the simulator, evaluations may be performed by the designers on static or dynamic models of the control system, in order to test certain design options. For example, several partial or targeted evaluations were performed by EDF on control room models of the Flamanville 3 EPR between 2002 and 2008, concerning subjects such as principles (display principles, etc.), presentation and organization of procedures, layout of the control room and arrangement of the backup process information and control system (equivalent to the auxiliary panel of earlier reactors).

Validation is based on an iterative approach, involving a succession of test campaigns. Where necessary, the lessons from one campaign result in changes that are tested during the following campaign.

In addition, validation does not only concern the main control room design, but extends to the remote shutdown station as well.

▶ Example of N4 series reactors

In the case of the control room for the N4 series reactors, IPSN asked, as part of its expert assessment, not only for the results of the assessments conducted by EDF but also to examine – as part of an agreement establishing the conditions of IPSN's involvement – the methods and tools planned to show that the design meets the objectives and options adopted, from a nuclear safety perspective. EDF remained responsible for choosing the procedure to be followed in conducting the assessments. IPSN made sure that the ergonomic assessments were conducted in conditions that guaranteed the validity of the data and analyses (choice of subjects, observation and data collection methods, operator profiles, choice of scenarios, etc.), using teams of assessors experienced in ergonomics. IPSN also examined the representativeness of the simulator relative to the real control room of the N4 series reactors[543].

[543] *Palier N4 : évaluation de la sûreté des aspects facteurs humains de la salle de commande informatisée* (The N4 Series: Assessment of Human-Factor Safety Aspects in the Computerized Control Room), Daniel Tasset, *Revue générale nucléaire*, No. 1, January-February, 1998, pages 20-26.

As indicated above, the conclusions of IPSN's evaluations conducted in 1994 led EDF to conduct additional targeted tests in 1995, a new integrated system test campaign on the S3C simulator in 1996, and ergonomic observations during on-site hot tests[544].

Finally, for the N4 series design, five successive test campaigns on the S3C simulator were performed by EDF from 1986 to 1996:

- the first test campaign, in 1987 and 1988, mainly concerned aspects related to the equipment and its use;
- the second campaign in 1989 concerned normal operation;
- the third campaign in 1994 concerned operator actions in incident or accident situations;
- additional targeted tests took place in 1995;
- the last test campaign, involving operator actions in incident or accident situations, was conducted in 1996.

Throughout these campaigns, IPSN monitored the preparation and performance of the tests, through technical exchanges with EDF and through additional observations conducted by its experts.

These tests examined various subjects, such as operator actions using the computerized operation system (KIC), operator actions at the auxiliary panel when there is a KIC failure, operator actions in the event of failure on one of the KIC components, and the organization and training of the operating crew.

▶ Example involving organization of operator actions for the N4 series reactors and the Flamanville 3 EPR

The organization of operator actions illustrates the benefits of test campaigns. The computerization of the control room led EDF to change the respective roles of shift supervisor and safety engineer in incident and accident situations (see chapters 32 and 33). This change was debated often between the operator and nuclear safety organizations concerning the roles and tools of the safety engineer in the control room. Designers of the N4 series reactors had planned for the safety engineer and the shift supervisor to share the same computer workstation in the control room. The results of the first integrated system tests showed that by sharing the workstation in this way, the safety engineer was viewing the same displays as the shift supervisor. As a result, the safety engineer was playing a significant role in the shift supervisor's activities, such that the engineer could no longer approach the safety of operator actions from a fully independent point of view. This led the Directorate for the Safety of Nuclear Installations to ask EDF to perform a comparative assessment of two options for the

[544] See Chapter 19 on reactor startup tests.

safety engineer: work at a dedicated computerized workstation, or use of the auxiliary panel and the plant overview panel.

The results of later tests, especially those conducted in 1994, led EDF to systematically assign the safety engineer to the auxiliary panel once an incident or accident operating procedure was initiated.

Regarding the role and tools of the shift supervisor, several difficulties were brought to light during the 1994 tests (the supervisor had problems visualizing changes taking place in the plant [process] state, or mentally following the sequencing in procedures, etc.). Some of these difficulties subsisted during later tests. This is why the shift supervisor's role and tools in incident or accident operation were studied in various ergonomic assessments conducted in 1995.

This example shows that the tests highlighted difficulties in organizing operating crews and tested various measures for improving incident and accident operation.

In principle, the design of the Flamanville 3 EPR control room followed the same approach of successive test campaigns. These campaigns also led EDF to modify the organization of operating crews. The state-oriented approach was adopted from the design of the incident and accident operating procedures. Operator guidance was automated. In the early 2010s, EDF planned that a single operator would perform operational tasks for the nuclear steam supply system and the secondary system using a single set of operating procedures, but the validation campaigns performed on a full-scale simulator led it to abandon this choice and keep the organization used in earlier reactors, where these actions were divided between two operators.

16.1.2.5. Assessments conducted during reactor startup and after commissioning

After startup tests and commissioning of a reactor, during its first operating cycle, when it is shut down for the first time for fuel reloading in the core, it is useful to collect operating experience feedback on the use of control systems and resources from the HOF perspective, in order to assess their appropriateness and verify the robustness of the organization implemented.

This operating experience feedback must of course be based on observations made during real operation, in addition to the results from test campaigns performed on a simulator.

As indicated above, in the case of the N4 series, the observations made during startup tests, then during the first operating cycle and the first shutdown for reloading of Chooz B1 resulted in lessons learned that highlighted certain issues that had not come to light during the simulator tests. The results of these observations led EDF to improve the computerized control system.

16.1.3. Project management and human and organizational factors engineering programme

To correctly implement an HOF approach in a design project, a sufficiently detailed programme describing this approach and its relation with other design fields should be developed early in design and implemented by designers. For the various phases of facility lifetime, this programme must indicate the human activities important to safety, in all areas of the facility where the personnel works. It must describe the analysis methods to be used to take into account HOFs for each activity involved. Programme organization and management must also be described.

For this purpose, the following must be included:

- programme objectives and scope;
- planned organization, management, and composition of the HOF teams, as well as the skills and experience required of their members;
- activities for incorporating HOFs and their relationship with engineering activities to ensure they are correctly integrated;
- roles and responsibilities of HOF specialists in the project (leaders, contributors, support, etc.); in particular, specialists who contribute to the design and those involved in validating the design (on a simulator, etc.) must be sufficiently independent;
- expected results of actions taken to include HOFs;
- expected results at the end of each step, etc.

Programme description and management must help designers identify the position of those in charge of incorporating HOFs within a design project, who must appear in the project organization chart. This programme should be established and implemented from the start of the project, even if it is not complete at this stage and the mobilization of the HOF teams differs depending on the step in question. HOF studies must take into account engineering constraints and produce results that can be used in the different phases of facility lifetime up to the dismantling phase. Similarly, engineering practices and processes must be adapted to incorporate HOF studies opportunely.

16.2. Considering human and organizational aspects when designing changes to nuclear power plants

Nuclear power reactors undergo changes (often engineering or documentation changes[545]) throughout their operational life, aimed at improving their performance in terms of nuclear safety or electricity generation. A few hundred modifications may be made to facilities as part of the periodic reviews associated with the ten-yearly

[545] General operating rules, operating procedures and instructions, test sequences, etc.

reactor outages (for example, as part of the fourth ten-yearly outage of the 900 MWe reactors). Some of these modifications may significantly transform operating practices, which must be indicated sufficiently early so that they are not a source of problems or errors. This means that incorporating the real operating requirements and the changes likely to be made to the organization and work practices is an important part of designing any modifications.

16.2.1. Importance of human and organizational factors in designing modifications

Certain modifications to a reactor have an impact on operation and maintenance activities. While changes aim to improve operating performance, whether in terms of productivity, safety, security, or protection of human health and the environment, the measures taken may nonetheless make the operators' work more complex. This may become apparent in the fact that the expected benefits of the change are difficult to attain or involve significant 'cost' for the human resources and organizations in place, at the risk of affecting the nuclear safety of the facility.

If the possible negative effects of a modification are not sufficiently identified during the change engineering phase, at best they will only appear during validation, or during initial implementation at the site, weakening the sociotechnical system and potentially nuclear safety.

This is illustrated by the following examples of changes that impacted operator activities.

In 1997, EDF decided to modify the method of determining the G3 calibration curve used to compensate for instantaneous variations in core reactivity resulting from power variations, without causing a power distortion. A new method for processing the measurements taken during a periodic test was intended to readjust this curve according to fuel burnup (from irradiation in the core) for 900 MWe and 1300 MWe reactors. The use of this new method led to an increase in significant events between 1998 and 2001. The decision to proceed with the change had not been preceded by an analysis of other related activities taking place in the field, and its implementation at facilities did not have sufficient support from the centralized corporate services of EDF.

Similarly, the switch in the 1990s from an event-oriented approach to a state-oriented approach (SOA, see Chapter 33) for reactors in service was not without problems (given the vast scope of changes) in terms of bringing the operating crews at certain facilities to learn and use new procedures, which called for extensive training. These difficulties became apparent when analysing various events where SOA procedures had been implemented[546].

[546] For example, at the Tricastin nuclear power plant (900 MWe reactors), in March 1999 on Unit 2 and January 2000 on Unit 1, as well as January 2002 on Unit 2 of the Flamanville nuclear power plant (1300 MWe reactor).

In this context, in 2004, safety organizations discovered weaknesses during an initial investigation into the integration of HOF aspects in the design of engineering and documentation changes to reactors in the French nuclear power plant fleet. The causes cited were, in summary, a lack of HOF skills in the teams in charge of the changes, insufficient dialogue between engineering and operational units, and the lack of scheduled HOF steps clearly integrated in the change engineering process.

Following this investigation, the Directorate General for the Safety of Nuclear Installations asked EDF to define and deploy a structured approach to considering the human and organizational aspects during the design of changes to reactors in the nuclear power plant fleet.

16.2.2. 'Human, social and organizational approach' implemented by EDF

In response, starting in 2007 EDF used in-house research and development to design and then implement an approach for taking into account human, social and organizational aspects (the 'HSO approach') within its engineering units to better control changes to facilities and their operating conditions.

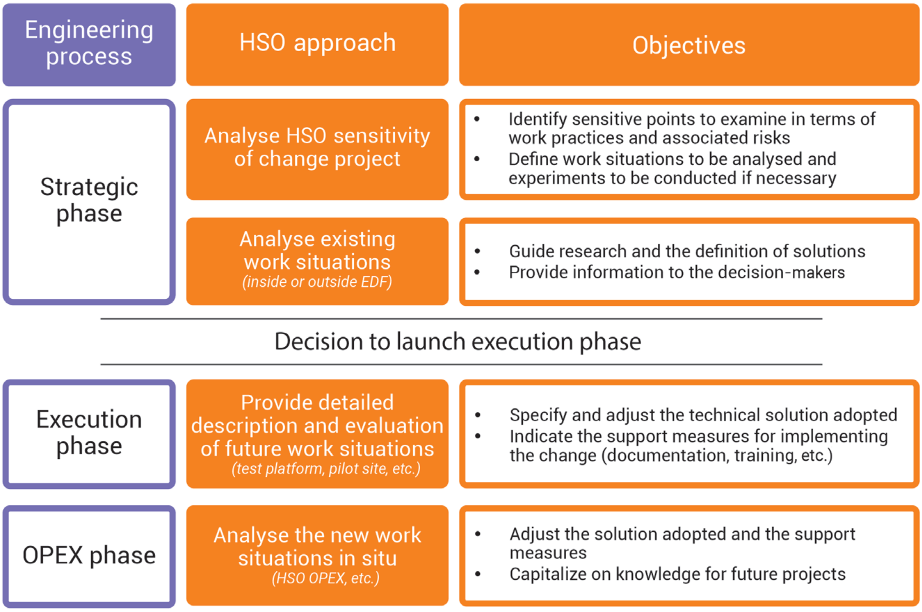
▶ Goal of the 'HSO approach'

The stated goal of EDF was to reap the expected benefits of the changes by taking into account the modified operating situations. This entailed identifying as early as possible any potential for degraded safety performance and taking any necessary action. More specifically, the HSO approach involves anticipating how an engineering or documentation change can lead to modifications in work practices in such a way that joint action can be taken on all aspects likely to influence the quality of work practices; in other words, providing the necessary means to carry out the relevant individual and collective activities, including aspects such as organization, training, documentation, work procedures and the physical work environment.

▶ Steps included in the engineering process of the nuclear power plant fleet

As illustrated in Figure 16.2 below, the HSO approach includes an analysis of the existing work situations, together with the identification and definition of possible solutions for achieving the objective of a change (indicating the cost, time frame, effects on documentation and operation, etc.).

Once a solution for the change has been selected, the process continues with a detailed design phase that leads to a detailed definition of the change. Before changes are applied in the power plant, an assessment of the planned measures, examined in detail, ensures that the expected results will be obtained. This is followed by implementation in a first-off plant unit to check the effectiveness (including the effect on work situations, procedures, etc.) of the change before any decision is made to extend it to other units. This analysis of the new work practices conducted in the workplace is used to compile operating experience feedback and proceed with any necessary adjustments.



Engineering process	HSO approach	Objectives
Strategic phase	Analyse HSO sensitivity of change project	• Identify sensitive points to examine in terms of work practices and associated risks • Define work situations to be analysed and experiments to be conducted if necessary
	Analyse existing work situations *(inside or outside EDF)*	• Guide research and the definition of solutions • Provide information to the decision-makers
	Decision to launch execution phase	
Execution phase	Provide detailed description and evaluation of future work situations *(test platform, pilot site, etc.)*	• Specify and adjust the technical solution adopted • Indicate the support measures for implementing the change (documentation, training, etc.)
OPEX phase	Analyse the new work situations in situ *(HSO OPEX, etc.)*	• Adjust the solution adopted and the support measures • Capitalize on knowledge for future projects

Figure 16.2. Steps taken in the approach to integrating human, social and organizational (HSO) aspects in planned changes, based on EDF diagrams. Georges Goué/IRSN.

Implementing the HSO approach includes a preliminary step to analyse the 'sensitivity' of a change in terms of HOFs. It should be noted that not every change project necessarily involves using the HSO approach. In addition, there are substantial differences in the type, extent and complexity of subjects to be considered.

For example, switching from the event-oriented approach to the state-oriented approach is a change that is extremely different from replacing an obsolete valve.

It is clear that, concerning changes to incident or accident operation, an HSO approach must be used because the changes affect individual and collective practices important to nuclear safety. In contrast, using a new valve model to replace an earlier model is a decision that does not immediately appear to have an impact on work practices.

In order to determine whether this change requires an HSO approach (analysis of 'sensitivity' in terms of HOFs), a few questions must be answered, such as:

– Who operates the valve? In what context? In what environment (ambient thermal conditions, overall dimensions, etc.)? With what frequency (daily, monthly, yearly)?

- Does operating the valve require coordination with other people in the field or in the control room?
- Does operating the new valve replace a prior activity or is it a new activity?
- If it is a new activity, is the workload it causes compatible with the other activities of the concerned individual or group?
- Does the valve directly affect nuclear safety?

According to the answers to these questions, changing the valve may have a variable degree of impact in terms of HOF.

The results of questions such as these must reveal the real-life work situations to be analysed and any need for simulation in order to identify the work situations that would result from the planned changes, taking into account the technical and organizational differences between nuclear power plants in France (while the French fleet is based on a limited number of standard plant units, the equipment associated with any given type of reactor may vary from one facility to another due to technological changes, and organizational situations may also differ).

▶ A support system

EDF provides methodological guides and one- to two-day training sessions for managers, project managers, engineers and technicians involved in designing changes and offers the opportunity to call on HOF specialists.

16.2.3. Changes, a subject that always deserves special attention from a human and organizational factors perspective

When IRSN conducted a new examination in 2009 of the system used by EDF, the nuclear safety organizations considered that the HSO approach had led to significant progress due to the quality of the methodological guides prepared by EDF and the effort made to incorporate the approach in engineering practices.

However, recurring weaknesses have still been found concerning the adoption of the HSO approach by the engineering centres charged with using it. Events in 2017 at the Tricastin and Chinon B facilities revealed shortcomings in the organization of EDF that prevented people from completely understanding the operating constraints that prevail during change projects.

The ageing of the nuclear power plant fleet, the anticipated extension of its operating lifetime, and the implementation of changes adopted following the Fukushima Daiichi nuclear power plant accident will lead to significant changes in equipment and documentation. As a result, controlling the design process and incorporating changes is a major issue for EDF, who needs to grant special attention to human and organizational aspects to successfully achieve this mission.

16.3. Human and organizational factors for future nuclear power reactor projects

The many changes made to nuclear pressurized water reactors over time on a case-by-case basis, especially as part of safety reassessments associated with ten-yearly outages, have aimed to take into account significant general lessons or major events such as the accidents at the Three Mile Island and Chernobyl nuclear power plants, and more recently at the Fukushima Daiichi power plant. These changes raise the question of the 'right' level of complexity in a facility[547].

The impact of increasing complexity is a subject of concern for which there has been few studies, but the subject is approached from a qualitative point of view in certain texts. In France, for pressurized water reactors, ASN Guide No. 22, cited previously, mentions that "the reasonably practicable (or non-reasonably practicable) nature of a given measure or of reaching a certain goal is assessed based on an overall analysis of the benefits to be gained in terms of nuclear safety and radiation protection in comparison to the industrial and economic costs in terms of increasing complexity in design or future operation, given the state of technology and the stage of project development. This assessment generally involves a timely examination of various solutions".

In its 2017 document[548] on the 'reasonably practicable' nature of improvements to existing facilities, pursuant to Article 8a of the 2014 European directive[549], the Western European Nuclear Regulators Association, WENRA, also underscored the risk of undue complexity in facility design or operation, which should be taken into account in decision-making processes.

The issue of increased complexity, of course, does not only concern changes in existing reactors, but also applies to the design of new facilities. It is one of the subjects of technical discussions between EDF and safety organizations pertaining to a certain pressurized water reactor project, initially called the New-Model EPR.

New reactor projects sometimes incorporate technological advances that may lead to important changes in facility operation, such as increased automation, which modifies the role, training, and experience gained by operators on a daily basis.

The case of Small Modular Reactor (SMR) projects may lead to investigations on various issues involving control room design and the organization of operating crews. Certain characteristics announced by the designers of this type of technology (use of

[547] On this subject, readers may wish to consult Normal Accident – Living with High-Risk Technologies by C. Perrow, Basic Books, 1984.

[548] WENRA Guidance – Article 8a of the EU Nuclear Safety Directive: Timely Implementation of Reasonably Practicable Safety Improvements to Existing Nuclear Power Plants – Report of the Ad-hoc Group to WENRA, 13 June 2017.

[549] Article 8a in the English version of the directive, 8b in the French version (Council Directive 2014/87/Euratom of 8 July 2014, amending the Directive 009/71/Euratom establishing a Community framework for the nuclear safety of nuclear facilities).

'passive' systems, increased automation, increased 'idle time' where operators have no action to take[550], etc.) have led to claims that facilities could be operated by smaller crews compared to nuclear power plants currently or soon to be in operation. In addition, it appears technically feasible to monitor and operate several modules from one control room. Reflection is focused on the number and allocation of operators according to the various operating states in a set of modules implemented under satisfactory safety conditions. A study published in the USA in 2012[551] noted that, while having one operator control several units simultaneously is common in the petrochemical industry, it is still a source of problems in the area of self-driving cars, as operators sometimes tend to focus on one unit to the detriment of others, or do not detect important changes (an effect referred to as 'change blindness').

In the field, outside the control room, new technologies could also lead to important changes in maintenance practices, such as visualizing text and images using specialized glasses, use of 'exoskeletons' (robots) to facilitate operations, etc. In theory, this type of change could improve nuclear safety significantly, but would probably raise new issues that designers and operators would have to resolve in a timely manner as part of their projects.

Finally, even more significant improvements in operation have been imagined by certain designers within a more or less distant time frame (such as the Flexblue project led by Naval Group as of 2008, then abandoned). For example, a reactor could have only a small number of operators on site (just the number required to oversee highly automated operations and occasionally perform minor maintenance operations and tasks), with other functions handled remotely by specialists that would come to the facility if necessary (for maintenance) or perform their tasks remotely.

[550] Also referred to as a 'grace period'.

[551] Human-Performance Issues Related to the Design and Operation of Small Modular Reactors, J. O'Hara, J. Higgins, M. Pena, NUREG/CR-7126, June 2012.

Chapter 17
Studying Core-Melt Accidents to Enhance Safety

A core-melt accident in a pressurized-water nuclear reactor is an accident during which the reactor fuel is significantly damaged with more or less extensive melting of the reactor core. Chapter 9, on loss-of-coolant accidents, describes a scenario liable to cause degradation to fuel rod cladding, but the protection and engineered safety systems can limit the extent of the damage. If, however, failures affect these systems, the accident may lead to core melt due to a prolonged absence of core cooling. Owing to the measures taken to prevent and mitigate the consequences of accidents, such an accident occurs only following a series of failures (multiple human errors or equipment failures).

In 1979, the accident in Unit 2 of the Three Mile Island power plant (see Chapter 32) in the USA showed that combinations of failures could lead to a core-melt accident. Fortunately, the environmental consequences of this accident were very limited due to the reflooding of the core after a few hours, preventing vessel melt-through by the molten core, and due to the containment, which performed correctly.

In 1986, the Chernobyl accident (see Chapter 34) illustrated the possibility of core destruction in a reactor when reactivity is excessive. It led to more in-depth study of the risk of reactivity accidents in pressurized water reactors, so as to determine additional measures, if necessary, to make them highly improbable, or even physically impossible. This subject is discussed briefly below, but will be developed further in Chapter 35.

In 2011, external hazards (earthquake followed by a tsunami), of a magnitude greater than that used to determine the height of the site's seawall led to core melt in several reactors of the Fukushima Daiichi nuclear power plant in Japan. This accident resulted in significant release of radioactive substances in the environment due to core melt in these reactors and subsequent containment failures.

While release to the environment caused by the Three Mile Island accident was ultimately very low, the plant management and the local and national authorities wondered for several days how the situation would turn out and if it would be necessary to evacuate people. In any case, in France and elsewhere the need to prepare for managing such situations was clear, despite the improved measures taken to avoid them.

If core degradation cannot be stopped inside a reactor vessel through cooling of the degraded core (by in-vessel reflooding), the core-melt accident may ultimately lead to a confinement failure and significant amounts of radioactive substances may be released to the environment. Because of the serious consequences of this kind of release, illustrated by the Fukushima Daiichi nuclear power plant accident mentioned above, significant efforts were made and continue to be made in the study of core-melt accidents, to better prevent them and mitigate their consequences.

The reactors for the various standardized series of the nuclear power plant fleet (900 MWe, 1300 MWe, and 1450 MWe reactors), for which the design bases did not include core melt, have been improved over time. Core-melt accidents are now taken into account in the design bases of new generation reactors such as the EPR.

In general, efforts have aimed to improve confidence in containment behaviour and containment behaviour itself, even in conditions very far from those used for its design. Another goal is to develop tools for predicting possible outcomes of the situation, the corresponding releases, and their transfer to the environment in the specific accident conditions, so that decision-makers can take the best decisions in a timely manner for protecting people and the environment. These are the subjects discussed in this chapter.

Before examining containment behaviour, it is useful to review the successive physical phenomena that may occur in a pressurized-water power reactor during a core-melt accident.

17.1. Core degradation and vessel failure

Since the Rasmussen Report, probabilistic safety assessments have shown the wide variety of scenarios liable to lead to core damage. However, it should be noted that although these scenarios can be triggered by different initiating events, they may lead to similar developments after core melt.

Understanding certain characteristics of the reactor state at the time of core uncovery is sufficient to determine the subsequent evolution of the accident. Examples of these characteristics include:

- **the instant at which the core-melt accident occurs**, as this determines the corresponding amount of decay heat in the core and thus the rate of progression of the accident;
- **the pressure in the reactor coolant system during the core-melt accident**: particularly accidents where an RHRS failure leads to high-pressure core-melt situations, which lead to specific risks of damage to the containment;
- **the state of engineered safety systems**, especially the availability of the containment spray system, which removes heat from the containment and removes airborne radioactive substances from the containment atmosphere;
- **the level of core subcriticality**;
- **the state of the containment (and its extensions)**: it may be isolated or bypassed (for example, due to a loss of coolant through a break outside the containment), or it may be subject to leakage (for example, when the equipment hatch fails to close).

Given the similarities that can be shown in this way in the expected progression of the various core-melt accident scenarios, it is possible to generically assess the various phenomena that may occur during these accidents. These phenomena are summarized below[552].

17.1.1. Core uncovery

As indicated above, multiple event 'scenarios' may lead to core melt in a pressurized water reactor core. To illustrate, this chapter will be limited to scenarios where the initiating event is a reactor coolant system break, the type of accident described in detail in Chapter 9.

Core uncovery begins when the fuel rods are no longer completely immersed in coolant due to a loss of reactor coolant.

Depending on the initial state of the reactor, the initiating event of the accident sequence, system failures and any operating errors, core uncovery can be reached within a matter of minutes, hours or days after the initiating event. Core uncovery leads to core melt only if sustained cooling cannot be restored rapidly enough.

For example, a 10 cm break in a pipe in the reactor coolant system would, if water is not injected by the safety injection system, lead to complete uncovery of the fuel rods in 30 min.

The situations resulting in prolonged core uncovery may be classified in various categories according to the pressure in the vessel at that time:

[552] Readers may wish to consult Nuclear Power Reactor Core Melt Accidents – Current State of Knowledge, D. Jacquemain *et al.*, Science and Technology Series, IRSN/EDP Sciences, 2013.

– breaks in the reactor coolant system (RCS) that lead to core uncovery at relatively low pressure, less than about 15 to 20 bars (order of magnitude);

– failures in RCS cooling via the secondary lines of the steam generators or mechanical failure in the vessel resulting from a pressure increase due to delayed reflooding of a degraded core, which lead to core uncovery under high pressure, above approximately 15 to 20 bars (order of magnitude).

The progression and consequences of the accident will vary depending on the pressure in the vessel at the time of core uncovery and the moment when mechanical failure of the vessel occurs. In practice, a high-pressure core-melt accident occurs when the vessel pressure is greater than approximately 15 to 20 bars at the time of failure.

17.1.2. Fuel degradation

The uncovered part of the core heats up under the action of decay heat.

At normal operation, the cladding surrounding the fuel is at a maximum temperature of 350°C. At temperatures of 700-900°C, the cladding becomes deformed due to the degradation of its mechanical properties.

If the pressure in the vessel is lower than the pressure in the fuel rods, the cladding swells until it bursts. If the pressure in the vessel is higher than the pressure in the fuel rods, the cladding pushes against the fuel pellets, inducing formation of a UO_2-Zr eutectic with a melting point of 1200°C to 1400°C.

In both cases, volatile fission products (FPs) that accumulate between the fuel pellets and the cladding are released in the reactor coolant system.

The zirconium in the fuel-rod cladding oxidizes in contact with the superheated steam. The oxidation reaction starts at about 1200°C and the reaction rate accelerates very quickly as the temperature rises, starting at about 1500°C. However:

– this reaction is highly exothermic and releases heat locally that is greater than the decay heat of the fuel. If cooling is unable to remove this heat, both the temperature of the materials and the oxidation reaction rate rise. This phenomenon is known as 'oxidation reaction runaway';

– the reaction releases hydrogen[553] into the reactor coolant system then into the containment (via the break); the presence of hydrogen reduces the cooling capacity of the steam generators, leading to a risk of hydrogen combustion or even explosion in the containment;

– the cladding is embrittled and more vulnerable to thermal shock.

[553] Oxidation of 1 kg of zirconium produces about 0.5 m^3 of hydrogen at normal temperature and pressure. Given the quantities of zirconium in the various types of facility, this represents production of about one kilogram of hydrogen per MWe.

Furthermore, the kinetics at which fission products are released from the fuel pellets increase as the fuel pellet temperature rises.

In summary, the main phenomena that occur with core damage are:

– between 900°C and 1800°C, melting or vaporization of the metal components in the core (control rod components, structural steel, non-oxidized Zircaloy in the cladding);

– above 1800°C, melting of other core components (oxides, etc.).

Temperatures of the order of 2800°C are required before the uranium oxide will begin melting. However, the presence of eutectic mixtures of uranium oxide, zirconium and steel may cause molten materials to relocate at lower temperatures. This causes a local then general collapse of the reactor core and the formation of 'corium', a molten mixture of fuel and structural materials, kept molten by the decay heat from radioactive decay of the fission products retained in the corium.

Nearly all of the most volatile fission products will have been released from the fuel at this point.

17.1.3. Failure of the reactor coolant system

▶ Vessel lower-head failure

Due to thermal-mechanical effects, the lower head of the vessel may fail within a matter of tens of minutes or hours following collapse of the component elements of the core. This interval depends on the corium mass in the lower part of the vessel, the heat released by this mass, and the presence or absence of water to remove part of this heat through evaporation.

▶ Rupture of reactor coolant system structures

During core melting, the hot steam exiting the reactor core and circulating by natural convection through the reactor coolant system causes the RCS structures to heat up excessively. If the RCS is pressurized, structures such as the steam generator tubes may undergo a phenomenon of creep, causing them to break (known as an 'induced' rupture, see below).

17.1.4. Phenomena that can cause early containment failure

▶ 'Induced' steam generator tube rupture

'Induced' rupture of the steam generator tubes would cause fission products to be released directly to the environment via the safety valves on the secondary loops (for example, the safety valves on the 900 MWe units are set to 76 bars).

Direct heating of gases in the containment

If the reactor coolant system is pressurized when the vessel fails, corium jet fragmentation may disperse corium inside the containment, producing a sharp rise in pressure as the heat in the molten corium is rapidly transferred to the gases in the containment atmosphere. This phenomenon is called ‘direct heating of gases in the containment’. It may also lead to combustion of the hydrogen present in the containment.

‘Hydrogen risk’

‘Hydrogen risk’ refers to the possible loss of containment integrity if hydrogen ignition occurs. As noted above, hydrogen is produced by oxidation of the zirconium in the fuel rod cladding as well as metal structures in the core during core degradation, and by oxidation of the metals in the corium or the steel rebars in the concrete basemat when the corium interacts with the concrete (see Section 17.1.5). This hydrogen builds up inside the containment and can locally reach high concentrations that exceed the flammability threshold in the H_2 + O_2 (air) + H_2O gas mixture (see Figure 17.1).

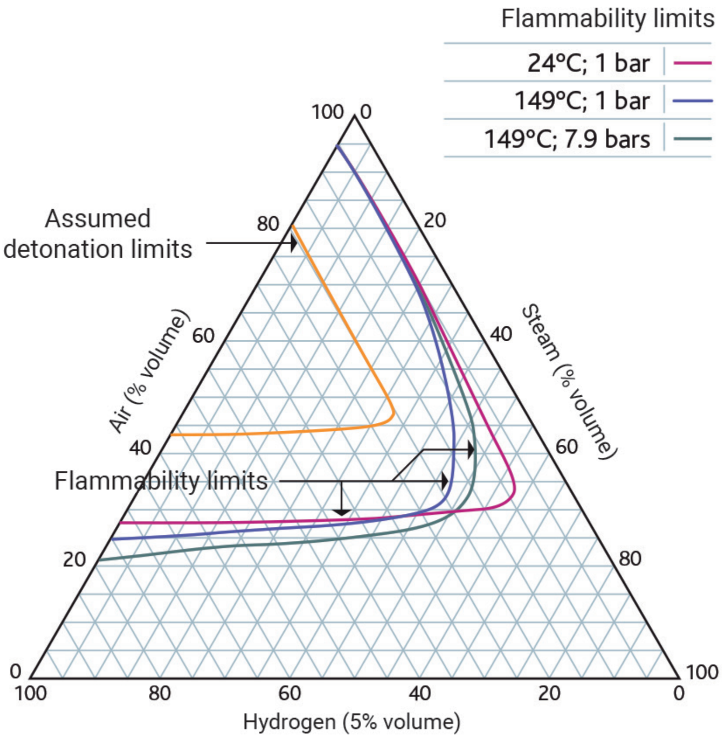


Figure 17.1. The Shapiro diagram, showing the flammability limits of a hydrogen-water-air mixture (the detonation limits were called into question by later studies). IRSN.

▶ Steam explosion

Corium may interact with water present in the vessel lower head (if the molten corium relocates here) or in the reactor pit (if the vessel lower head is breached). As the corium is at a much higher temperature than the water, this contact can trigger a very energetic thermodynamic interaction. On contact with the water, the corium may be highly fragmented and cause massive, instantaneous vaporization of the water. This phenomenon is known as a 'steam explosion'.

▶ Other cases

It is also interesting to note the case of pre-existing containment failures, which can lead to significant early releases (as when the seal is defective on a containment penetration).

17.1.5. Phenomena that can ultimately lead to containment failure

When corium comes into contact with the basemat concrete in the reactor pit, the concrete breaks down due to the heat released by the corium.

This gradually erodes the basemat, incorporating concrete components in the corium (such as calcium oxides and silica) and producing carbon gases, mainly carbon monoxide and carbon dioxide. Hydrogen can also be produced through oxidation of metal materials not yet oxidized in the corium or from melting of the metal rebars in the basemat concrete. The interaction between corium and concrete thus contributes to the risk of confinement failure by basemat cracking or melt-through (if the basemat is significantly eroded) and to the risk of combustion through the production of hydrogen and carbon monoxide (also a flammable gas).

For French reactors, the assessments of basemat melt-through kinetics for the various reactors, taking into account the basemat concrete thickness and composition type (silica or calcium-silicate concrete), made it possible to assume, based on knowledge available in 2015 pertaining to corium-concrete interactions, that there would be no basemat melt-through before 24 h – including for the two Fessenheim units whose basemats were thickened (see Section 30.4.5). However, in 2019, as part of the review of studies presented by Électricité de France (EDF) on mitigating core-melt accidents, subsequent to deployment of the post-Fukushima changes, IRSN found that, given available knowledge, uncertainty remained regarding the complex phenomena governing corium stabilization in basemats made of very siliceous concrete, which are still being investigated in important research projects.

17.2. Containment failure modes

As indicated in Chapter 14, professor Norman C. Rasmussen at the Massachusetts Institute of Technology was asked by the US nuclear safety authority to direct a scientific study (1972-1975) on the risks of using nuclear power reactors (pressurized or boiling water reactors), and then compare the results with other sources of risk for the public (such as meteorites). This study gave a systematic analysis of possible accident scenarios. The report's general conclusions were given as graphs showing the relationship between accident probabilities and 'expected' numbers of cancer fatalities.

Published in 1975 under the reference numbers WASH 1400 and NUREG 75-014, the Rasmussen Report is the first example of a comprehensive probabilistic safety assessment (PSA) giving figures for the probable impact on the population (Level 3 PSA).

In the report, Rasmussen introduced a classification of the possible containment failure modes (Figure 17.2) that is still in use today. There are five main modes:

– **α mode**: involves steam explosion in the vessel or reactor pit, caused by an interaction between corium and coolant water, inducing containment failure in the short term;

– **β mode:** involves initial or rapidly induced containment failure;

– **γ mode:** involves hydrogen explosion in the containment, leading to containment failure;

– **δ mode:** involves slow overpressurization of the containment, leading to containment failure;

– **ε mode:** involves basemat erosion by the corium, inducing basemat melt-through and thus containment failure.

The V mode, which corresponds to bypass of the containment by outgoing pipes, is dealt with separately, since it is not the direct result of building behaviour.

With the exception of the β mode, the scenarios above leading to containment failure correspond to more or less long-term core-melt accidents, resulting in the mechanical failure of the reactor vessel.

Other failure modes were identified after the Rasmussen Report was released; for example, in the early 1980s, the possibility of containment failure due to 'direct heating of gases in the containment' (see above).

The Rasmussen Report immediately began to be used for nuclear safety in French reactors in 1975. The first applications mainly focused on finding ways to mitigate the consequences of core-melt accidents. But following the Three Mile Island accident, the need to conduct an in-depth study of the provisions and means required to manage a core-melt accident was recognized as essential. The adopted approach first involved short-term implementation of provisions and means to improve prevention of core-melt accidents and mitigate the consequences. Then studies and R&D work were conducted to improve knowledge of the physics of this type of accident[554].

[554] Readers may also wish to consult Current State of Research on Pressurized Water Reactor Safety, Chapter 5, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, April 2017.

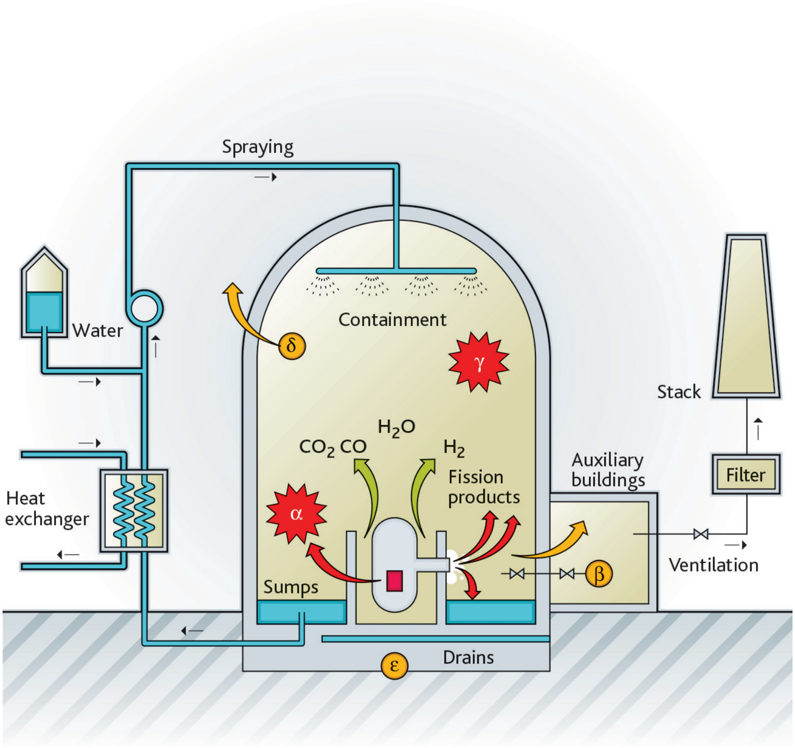


Figure 17.2. Schematic diagram of the possible containment failure modes (initiating event: reactor coolant system break) according to the Rasmussen Report. Georges Goué/IRSN Media Library.

These provisions and means included the implementation of specific procedures referred to as the 'H' (hypothetical) procedures (to prevent core melt) and the 'U' (ultimate) emergency procedures (to mitigate the consequences of core melt[555]), as well as reorganization of operation, improvements in reporting operating experience, and the development of simulation tools and other resources that could be used in emergency situations.

A better understanding of containment behaviour in conditions significantly different from those adopted in the design basis – which is determinant for the consequences of a core-melt accident – was quickly recognized as essential in making timely decisions to provide the best possible protection for people and the environment, as were tools for simulating possible sequences of an accident situation, the corresponding releases, and their transfer to the environment.

EDF as well as IPSN conducted studies (see Chapter 14) to:

[555] The various U procedures are discussed in Section 17.8 and in Chapter 33 with regard to incident and accident operation.

– investigate the possible containment failure modes and determine the resources required to address them under the best possible conditions,

– determine the environmental releases corresponding to different core-melt reference accidents (see next section).

The lessons learned from this work led EDF to take specific measures in reactors (such as blocking passages in the reactor pit and installing the 'sand filter' associated with the U5 procedure). They also served as the basis for writing Severe Accident Operating Guidelines for each reactor series. These guidelines describe the specific actions to be taken in the event of a severe accident to ensure the best possible confinement of radioactive substances for as long as possible (passing from a core-melt prevention objective to a sustained confinement objective).

As for the French authorities, they studied and set up systems for the protection of the public around nuclear sites – described in the off-site emergency plans[556] – in addition to the general provisions related to the ORSEC plan[557] (see Chapter 38).

The 2011 accident at the Fukushima Daiichi nuclear power plant, which resulted in core melt in three reactors with significant releases, led to an in-depth reassessment of the effectiveness of the measures already taken to prevent and mitigate the consequences of a core-melt accident in French reactors. Action was also taken to strengthen these measures, with a particular focus on accidents likely to occur in buildings containing fuel storage pools. This reassessment is discussed in detail in Chapter 36.

17.3. Classification of releases associated with core-melt accidents – 'source terms'

Based on the Rasmussen Report, IPSN identified typical releases[558], which they referred to as 'source terms'. A source term is a specific type of release (to the atmosphere) characteristic of a family of reactors and representative of a given type of accident, in general a containment failure mode following complete core melt. The source term is taken into account when defining planned actions to protect the public in these conditions.

Three source terms, listed in decreasing order of severity, were defined:

– **source term S1** corresponded to short-term containment failure occurring no more than a few hours after the onset of the accident;

– **source term S2** corresponded to direct releases to the atmosphere following containment failure one or more days after the onset of the accident;

[556] *Plan particulier d'intervention*, PPI.

[557] Civil protection plan.

[558] The studies were underway when the Three Mile Island accident occurred.

– **source term S3** corresponded to indirect, delayed releases to the atmosphere through pathways allowing a significant amount of fission products to be retained.

Using the Rasmussen classification, the α, β, and γ modes could lead to type S1 releases. The δ mode could lead to type S2 releases. The ε mode, containment failure due to basemat melt-through, could lead to type S3 releases because they would be filtered by the ground under the basemat before being diffused in the atmosphere.

The following table provides the orders of magnitude for releases associated with the three source terms for a 900 MWe reactor, as assessed in the 1980s.

Table 17.1. S1, S2, and S3 source terms for a 900 MWe PWR expressed as percentages of the initial activity of the radioactive substances present in the reactor core.

Source term	S1	S2	S3
Noble gases	80	75	75
Inorganic iodine	60	2.7	0.3
Organic iodine	0.7	0.55	0.55
Caesium	40	5.5	0.35
Tellurium	8	5.5	0.35
Strontium	5	0.6	0.04
Ruthenium	2	0.5	0.03
Lanthanides and actinides	0.3	0.08	0.005

The S3 source term was partially updated at the end of the 1980s, taking into account new knowledge and after U procedures had been introduced for French reactors, notably the U5 procedure associated with a system for reducing pressure in the containment in the event of an accident. This system consists of a venting line equipped with a sand filter, which was later equipped with a metal pre-filter in the containment to limit radioactivity in the sand filter, which otherwise could lead to radiation protection problems on site and cause the sand filter to heat up.

At the end of the 1990s, a delayed, filtered release via the sand filter was agreed upon for representing the reference S3 source term. This release is assumed to spread somewhere between 24 h and 48 h after the onset of the accident. It served as the technical basis for the off-site emergency plans.

The radiological consequences associated with the S3 source term are explained later on, in Section 17.7, as well as the relationship of this source term with the definition of provisions adopted in the off-site emergency plans. The radiological consequences mainly depend in the short term on iodine release and in the long term on caesium release. In practical terms, iodine release ‘governs’ the measures to be taken in the short term to protect the public, while caesium release ‘governs’ the medium- and long-term measures.

17.4. Improving knowledge

Since the Three Mile Island accident, many experimental results have been obtained internationally concerning the phenomena associated with a core-melt accident[559]. France (including IRSN) played an important role in obtaining these results, particularly through the Phébus-CSD and then the Phébus-FP programmes, which were conducted at the Cadarache nuclear research centre. Knowledge and understanding of the complex phenomena involved in such accidents have grown considerably. Likewise, the ability to predict changes in the reactor state through the use of simulation tools has significantly improved.

Knowledge in this area continues to evolve, for example with regard to iodine behaviour in the reactor coolant system and the containment, or the filtration systems that can be used during a core-melt accident. Significant research programmes have been defined internationally that aim, in the 2020s, to improve measures taken to reduce release and to develop tools capable of predicting release more accurately, thereby improving the management of actual accident situations.

17.5. Studies in France on containment failure modes

17.5.1. Introduction

After the definition of source terms, studies conducted in France following the Rasmussen Report sought to identify provisions for strengthening the last confinement barrier of the French nuclear power plant fleet, given the various failure modes possible for containments.

These studies were conducted with realism in mind. The aim was not to provide a ‘demonstration’ based on conservative assumptions, but rather to pragmatically find ways to improve facilities that have a given basic design and to define procedures for protecting the population under the best possible conditions – even if these improvements and procedures could require the implementation of additional equipment.

Thus, following the accident at the Three Mile Island plant, ‘ultimate emergency’ procedures (U procedures) and additional provisions were gradually implemented for all units in the French fleet to avoid or reduce the radiological consequences of a core-melt accident. EDF’s Severe Accident Operating Guidelines[560] recommend specific actions to be implemented under the control of emergency response teams, notably the emergency procedures mentioned above, when required by the accident situation to ensure adequate confinement of radioactive substances.

[559] See Current State of Research on Pressurized Water Reactor Safety, Chapter 5, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, April 2017.

[560] Which are not, strictly speaking, operating procedures.

17.5.2. Initial containment leakage

During normal operation, overall containment integrity is continuously monitored by a system that is based on pressure measurements, capable of detecting a large leak (open airlock or penetration). Moreover, the devices used to isolate containment penetrations are periodically and individually tested to ensure that they provide a leaktight seal. Lastly, the containment is pressurized at reactor startup (before fuel is initially loaded into the core), then once every ten years, to check that the total containment leak rate complies with technical requirements. All these checks are conducted to assess containment leakage and avoid the presence of any large leaks.

It is particularly important to avoid direct leaks (i.e. uncollected leaks, released directly to the environment without any time delay and without filtration), given their radiological consequences. During a core-melt accident, direct leaks can occur, for example, if automatic isolation of the various penetrations fails or if there are leaks in the airlocks. This confinement failure mode, referred to as the 'β mode', may lead to direct release of radioactivity to the environment practically from the beginning of the accident. 'Satisfactory' protection of the public in nearby areas from this release may not be assured in every case.

To manage this situation, EDF developed the U2 procedure entitled Action to Take in the Event of a Containment Isolation Fault. This procedure defines the conditions for monitoring containment integrity in an accident situation once a certain amount of radioactivity is present (even if it is not a core-melt accident), and the conditions in which any leaks are detected and located to correct them, if possible. The U2 procedure is implemented in addition to continuous monitoring for containment leaks that functions during normal operation, which can only detect very large leaks.

The U2 procedure encompasses:

- the conditions for monitoring confinement by measuring activity released by the stack, as well as activity in the containment, in the sampling systems of the reactor coolant system, and in the sumps in the peripheral rooms of the containment;
- actions to be taken, such as confirming that isolation commands have been carried out, locating leaks and implementing means to eliminate them, ensuring confinement of rooms, and, when the situation is under control and certain containment penetrations can be reopened, taking liquid effluent collected from peripheral buildings and re-injecting it into the reactor building.

17.5.3. Direct heating of gases in the containment

The main risk associated with this phenomenon – resulting from vessel failure under pressurization (melt-through by the corium) – is containment failure due to a rapid pressure increase within the building. This pressure increase is apparently caused by fragmentation and dispersion of corium in the containment, which could cause the gases inside to heat up and could trigger hydrogen combustion.

Preventing direct heating of the containment involves reducing the possibility of core melt under pressurization. This ultimately involves planning to intentionally reduce the pressure in the reactor coolant system so that the pressure in the vessel is below 15 or 20 bars (order of magnitude) when it fails.

17.5.4. Hydrogen explosion in the containment

Combustion of all the hydrogen produced by oxidation of the zirconium cladding in the 'active part' of the core (amounting to 80% of the total mass of zirconium in the core) would produce a pressure peak that could affect containment integrity.

To address this risk, in the early 1990s IPSN pointed out the advantages of equipping reactors in the nuclear power plant fleet with devices such as passive catalytic recombiners[561], that cause hydrogen to recombine with air (in the presence of steam, if necessary[562]), thus avoiding the combustion condition. At this stage, EDF was focused on finding a realistic demonstration of containment integrity in hydrogen explosion conditions, especially in 900 MWe reactors with a steel liner.

Passive catalytic recombiners contain plates made of a catalytic material (platinum or palladium) installed in a metal box that ensures gas circulation between the plates (see Figure 17.3). On contact with these catalytic recombiner plates, the hydrogen and oxygen present in the containment atmosphere react to produce steam.

Finally, after long discussions, all the units in the nuclear power plant fleet were gradually equipped with hydrogen recombiners[563]. The decision was made after convincing results were obtained, following a qualification process led by the manufacturers involving operation of these devices in core-melt accident conditions. It was supported by the results of national and international research programmes on the 'hydrogen risk' – in which IPSN participated[564]. The recombiners installed in the containment of pressurized water reactors are thus designed to operate in pressure, temperature, and humidity conditions and in a radioactive environment corresponding to severe accident conditions. The qualification of this equipment takes into account the risk that the catalytic plates will be contaminated by aerosols from the molten

[561] Previously, EDF considered bringing recombiners to the site of a reactor accident and connecting them to the containment atmosphere monitoring system (which monitors the hydrogen content in the air and stirs air inside the reactor building).

[562] Generated by the break and activation of the containment spray system.

[563] Igniters were also considered for the containment (in particular, a combination of igniters and recombiners was recommended in Germany by experts at the RSK), but this was not the solution adopted in France given the risks it entails. Igniters are active systems that burn hydrogen at low concentrations, before flammability limits are reached, so that spreadable flames are not produced. However, in certain conditions, hydrogen may accumulate to form a flammable mixture in the absence of water that may catch fire and produce flames that propagate and threaten the containment structure and the equipment required to manage a severe accident.

[564] Under the direction of the OECD and as part of the SARNET project. On this subject, readers may also refer to Section 5.2.2 of Nuclear Power Reactor Core Melt Accidents – Current State of Knowledge, Science and Technology Series, IRSN/EDP Sciences, 2013.

core and by boric acid coming from the potential activation of the spray system. Hydrogen recombiners were also installed in the nuclear power plants of neighbouring countries.

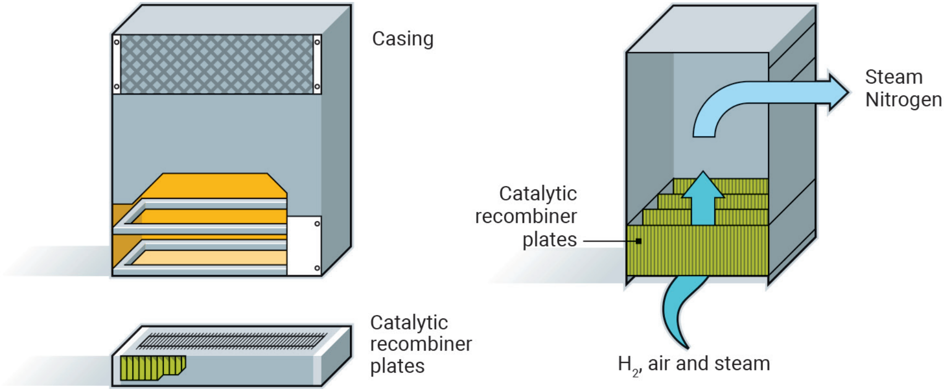


Figure 17.3. Block diagram of a passive catalytic recombiner. The catalytic plates (right) are positioned vertically in the components installed in horizontal drawers (left). Ahmed Bentaib/IRSN Media Library.

While this measure significantly reduced the probability of hydrogen combustion, which could affect containment integrity, it does not totally rule out this type of combustion. That is why this phenomenon continues to be studied and researched to find technical explanations that provide a better understanding of the risk associated with confinement failure and then develop new systems, as necessary.

17.5.5. Steam explosion in the vessel or reactor pit

A steam explosion may occur if hot, fragmented corium comes into contact with water present in either the vessel lower head of the reactor or, after vessel failure, the reactor pit (water from the break and from spray system activation).

The mechanical energy of a steam explosion in the vessel (associated with shock waves and expansion of the steam bubble) could cause the vessel to burst and generate projectiles that could endanger the integrity of the containment and particularly the vessel head. The α mode, as defined in the Rasmussen Report, corresponds to an in-vessel steam explosion that leads to vessel rupture and tears away the vessel head.

Concerning this type of steam explosion in the vessel, mechanical studies in various countries have led to the conviction that a direct failure of containment integrity induced by the α mode is highly unlikely.

The mechanical energy released by a steam explosion induced by corium flowing into a flooded reactor pit could compromise the strength of the structures adjacent to the reactor pit (particularly the adjoining walls and floors) as well as the strength of the various components of the reactor coolant system, and especially the containment.

To eliminate the risk associated with a steam explosion in the reactor pit, EDF studied measures that would keep the reactor pit dry until vessel failure occurred and the flow of corium spread into the reactor pit and adjacent areas. These provisions were defined and implemented as part of the periodic review associated with the fourth ten-yearly outage of 900 MWe units. Similar provisions will be examined as part of the next periodic reviews of 1300 MWe and 1450 MWe units. The case of the EPR is covered in Section 17.10.3.

17.5.6. Gradual pressure increase in the containment

The δ mode corresponds to containment failure from overpressure due to heating of the containment atmosphere caused by insufficient removal of the heat generated by fission products. This overpressure also results from the gradual formation of a very large amount of gas during erosion of the basemat concrete by corium. These gases may be accompanied by steam from the water used to cool the corium in an attempt to slow its progress.

If the containment atmosphere is not cooled, internal pressure will naturally rise, which could lead to containment failure after a period of 24 h.

In response to the possibility of irreversible containment failure, it was considered important to have a means of controlling the pressure inside the containment by allowing filtered releases.

The adopted solution consisted in using a containment penetration intended to vent pressure from the containment during its initial and subsequent periodic pressure tests. Referred to as ‘filtered venting’, the installed system consists of a set of valves, a relief valve and a filter housing with a 42 m^2 sand bed that is 80 cm thick. The system is fitted outside the containment between the penetration and the stack.

The requirements set for the containment filtered venting system were to ensure the following:

- limit then reduce pressure inside the containment,
- reduce aerosol activity in the released gases by a factor of at least 10,
- direct the filtered gases to the stack, where their activity was measured.

The filtration efficiency and geometry of the sand bed were tested and the flow conditions through the bed were optimized in the early 1990s by IPSN in its Cadarache research facilities in cooperation with EDF. These studies, which aimed to qualify the filters for severe accident conditions, showed it was possible to obtain or exceed the minimum desired efficiency (achieving a reduction factor of 10 for aerosols). The FUCHIA tests, performed using full-scale filters, showed a sand bed filtration efficiency that exceeded the minimum desired efficiency for aerosols by one order of magnitude.

Nonetheless, during later studies it was observed that if an accident were to occur, the build-up of radionuclides in the filter sand could lead to problems involving on-site radiological protection and filter heating. Furthermore, rapid condensation of water vapour in the pipes could cause a hydrogen deflagration (where the air/hydrogen/steam mixture leaving the containment becomes explosive due to the rapid decrease in the steam concentration). Various complementary measures were thus taken, one of which consisted in adding a pre-filter to the filtered venting system inside the containment to filter aerosols[565], while another entailed a system for heating the line outside the containment upstream of the sand filter. The pre-filter limited radioactivity in the sand filter, whereas heating the line avoided the anticipated steam condensation.

If a core-melt accident were to occur in a reactor, the containment filtered venting procedure (U5) would be implemented on site only in close cooperation with public authorities. The filtered venting system should be opened no earlier than 24 h after the onset of the accident. The purpose of this period is to allow the concentrations of radioactive substances in suspension inside the containment to decrease sufficiently before being released, and to allow enough time to implement measures to protect the public (preventive evacuation, sheltering) in proportion to the expected level of release to the environment.

Research continues on the filtration of fission products. Special attention is given to filtering gaseous species of iodine, especially organic iodides, to reduce the short-term radiological consequences of an accident. Studies focus on improving existing filtration systems as well as developing innovative filtering media.

17.5.7. Penetration of the concrete basemat of the containment by corium

The ε mode corresponds to a containment failure induced by corium penetration of the concrete basemat.

Based on the current state of knowledge from research on corium-concrete interaction, corium erosion of the concrete basemat, in the absence of corium cooling, could lead to total penetration within a time interval that varies depending on the basemat characteristics (type of concrete[566], basemat thickness[567]), but is greater than 24 h for all basemats of the 900 MWe, 1300 MWe and 1450 MWe units[568].

As part of the periodic review associated with the fourth ten-yearly outage of 900 MWe units, EDF set an objective of avoiding basemat penetration in the event of a core-melt accident and proposed to implement appropriate measures. These measures consist of cooling the corium by flooding it with water after it has spread throughout the reactor pit and into an adjoining area. In order for corium to spread according to design expectations, no water must be present in the reactor pit and the adjacent area.

[565] The pre-filter and sand filter achieve a reduction factor of 1000 for aerosols and 10 for gaseous molecular iodine.

[566] Calcium-silicate, silica, or high-silica concrete.

[567] For the Fessenheim nuclear power plant units, the concrete basemat was thickened by EDF, bringing the corium penetration time to more than 24 h, with corium spreading in the reactor pit and an adjoining area.

[568] Uncertainties remain, however, as indicated in Section 17.1.5.

EDF recommends implementing an operating procedure that keeps the reactor pit dry until the corium has flowed down into the pit after vessel failure, which would also avoid the risk of steam explosion in the reactor pit[569].

Furthermore, in the 2000s, IRSN began investigations on measures ('waterborne release countermeasures'[570]) that could be implemented preventively to keep highly contaminated water in the sumps from reaching underground water, then spreading to a nearby river or the sea, in the event of corium penetration of a basemat. These measures could be adapted to each site, combining a static barrier (such as a geotechnical enclosure under the reactor building) with dynamic confinement (a system for pumping and treating recovered water). As part of preparing a potential accident management scheme, analyses and studies could examine how the contaminated water would be treated.

17.5.8. 'U4' provisions

The initial basemat design of EDF nuclear power plants includes a network of drain pipes and penetrations (particularly for the basemat monitoring systems). Construction measures were therefore taken to prevent direct releases of gas and aerosols in the environment in the event of basemat erosion by corium (blocking these drains and penetrations with mortar or sealing pipes that had not initially been closed off with appropriate metal plugs welded on the ends).

The units at the Cruas site presented a specific challenge. Each unit rests on an upper basemat that is connected to a lower basemat by anti-seismic bearings. The empty space between these basemats is connected to the outside air and, in the event of a core-melt accident, could lead to the release of gas and unfiltered aerosols to the atmosphere. This led EDF to take specific measures ('U5 - Cruas' and 'U4 - Cruas') to avoid this kind of release. These provisions entail:

- venting the pressure inside the containment until it equals the pressure in the space between the basemats at the moment the corium penetrates the upper basemat, so that the contents of the containment atmosphere are not 'ejected' into this space,
- completely flooding the space with water to reduce releases to the environment under the resulting effects of dilution, filtration and cooling, and adding sodium hydroxide to this water to obtain an alkaline solution that will dissolve any iodine in the water.

17.5.9. Bypass of containment by outgoing pipes (the V mode)

Loss-of coolant-accidents with containment bypass, known as V-LOCAs, occur when coolant is lost through a break outside the containment in a loop connected

[569] The corium would spread in the bottom of the reactor pit and in the area adjacent to the instrumentation and control system equipment, leading to destruction of a 'fusible wall'.

[570] 'Waterborne release countermeasures' have been considered since the 1990s as part of reflections on how to manage a post-accident situation following core melt.

to and not isolated from the reactor coolant system. V-LOCAs have two specific characteristics:

– since coolant is lost outside the containment, it is not possible to recirculate the safety injection system water;

– in the event of core melt, fission products would be released directly outside the containment if the break is not isolated in time.

To prevent a containment failure due to a V-LOCA, EDF implemented design and operation changes on all the units in the French fleet. In particular, these changes addressed the risk of containment bypass in the event of a break in the thermal barrier of a reactor coolant pump and the portion of the system that cools this pump. These changes are designed to 'practically eliminate' V-LOCAs that might lead to significant early releases.

17.5.10. Fast reactivity insertion accidents

Fast (and significant) reactivity insertion accidents in the core of a pressurized water reactor mainly involve[571] inadvertent transfer of a 'plug' of insufficiently borated water to the core. These accidents, called 'heterogeneous dilution' accidents, may result from operator errors, malfunctions in auxiliary systems, or leaks in steam generator tubes, and are analysed in detailed studies.

The French studies of these scenarios, conducted following the 1986 accident at the Chernobyl plant, are discussed in Chapter 35 of this book.

17.6. Severe accident operating guidelines

For reactors in the French nuclear power plant fleet, the Severe Accident Operating Guidelines, written by the operator, aim to provide assistance to EDF's emergency response teams to ensure the best possible confinement of radioactive substances for as long as possible. These guidelines describe possible actions and recommendations to mitigate the consequences of a severe accident. These actions and recommendations are discussed by experts from EDF and IRSN to take into consideration advances in knowledge of severe accidents.

Once implementation of the Severe Accident Operating Guidelines has been initiated[572], priority is given to 'safeguarding' the containment rather than the reactor core.

Implementing the Severe Accident Operating Guidelines means that the operating crew abandons the accident operating procedures underway. Responsibility is then transferred from the operating crew to the emergency response teams. The Severe

[571] The ejection of a rod control cluster assembly (RCCA) is studied as a Category 4 accident operating condition and the reactor protection system is designed to mitigate this event.

[572] Main implementation criterion: the temperature of gases at the core outlet must exceed 1100°C.

Accident Operating Guidelines provide EDF's emergency response teams with the guidance they need to identify the best strategy for using available systems to safeguard the containment. The operating crew implements the operating actions requested by the local emergency response team.

Specific instrumentation is or will be set up during the ten-yearly outages of French reactors in operation, so that EDF emergency response teams can better assess the development of a core-melt accident and better inform authorities of the accident's progression (detection of hydrogen in the containment, detection of corium reaching the basemat in the reactor pit).

17.7. Radiological consequences associated with the S3 source term and emergency response plans implemented by public authorities

In the early 1980s, French public authorities explored the realistic possibilities of implementing measures to protect people (through sheltering and/or evacuation) located in the vicinity of French nuclear sites. Based on the characteristics of these sites, French authorities estimated that evacuating people within a 5 km radius of a site and sheltering people within a 10 km radius of a site would be possible within 12-24 h of the onset of an accident. They observed that implementing these measures would ensure a satisfactory level of short-term public protection against releases corresponding to the S3 source term as assessed at the time, given the response levels recommended by international organizations.

Off-site emergency plans were then defined on this basis.

Later reassessment did not lead to any changes in these plans (as seen in Section 17.3, the updated S3 source term corresponded to releases discharged through the containment filtered venting system to depressurize this structure 24 h after the onset of the core-melt accident[573]).

The radiological consequences were calculated based on weather conditions. The results are expressed in terms of effective doses from the radioactive plume (external and internal exposure), ground fallout, and ingestion and in terms of equivalent doses to the thyroid (primarily due to iodine). The doses received by humans are estimated using dose coefficient values (defined in documents published by the International Commission on Radiological Protection, ICRP). The results were assessed in light of the applicable public safety measures.

Public safety measures that may be implemented during the emergency phase are indicated in the off-site emergency plans, prepared by the prefects. The prefect may consider various public safety measures, including:

[573] Release is assessed for an accident with rapid kinetics, a large reactor coolant system break, and failure of the safety injection and containment spray systems.

- sheltering;
- ingestion of potassium iodide (stable iodine) to saturate the thyroid gland and avoid the fixation of radioactive iodine. On the prefect's orders, those liable to be affected[574] by radioactive iodine releases take the prescribed dose of potassium iodide. This measure is most effective when potassium iodide is ingested two hours before exposure to release;
- evacuation.

In 2007, in ICRP Publication 103, then in 2009 in ICRP Publication 109, ICRP released recommendations on protecting the public in an accident situation.

In France, a decision of the French Nuclear Safety Authority, ASN, from August 2009, 2009-DC-0153, which was approved by an order of the Minister of Health on 20 November 2009, set the response levels applicable in a radiological emergency situation to:

- an effective dose of 10 mSv for sheltering,
- an effective dose of 50 mSv for evacuation,
- an equivalent dose to the thyroid of 50 mSv for potassium iodide administration[575].

These levels are not thresholds, but are intended to guide public authorities in defining and implementing actions to protect the public in the event of an accident.

For the updated S3 source term (see Section 17.3), IRSN determined that the doses for the most radiosensitive members of the public could remain above 50 mSv up to 6 km and above 50 mSv to the thyroid up to 18 km, for 'average' weather conditions[576] and along the wind axis, assumed constant. As a result, measures already defined to ensure short-term protection of the public as part of the off-site emergency plans seemed fairly 'satisfactory' for a release at the level of the S3 source term.

Independently of their immediate radiological consequences, the Chernobyl nuclear power plant accident and more recently, the Fukushima Daiichi nuclear power plant accident, highlighted the significant social and economic disorder induced over the long term, due in particular to the contamination of land and food chains.

The nuclear accident at the Fukushima Daiichi nuclear power plant led public authorities to revise actions to protect the public, in line with international practices and recommendations from the European nuclear safety and radiation protection authorities. In April 2016, the French government (through the Ministry for the Environment) decided to enlarge the planning zone (the off-site emergency plan radius) around nuclear power plants from 10 to 20 km. This was not related to any rise in

[574] Newborns, children, adolescents and pregnant or nursing women are particularly sensitive.

[575] The level that had been used previously for the preventive distribution of stable iodine was 100 mSv to the thyroid.

[576] Normal diffusion and wind velocity of 7 m/s.

nuclear risk, but made it possible to better inform and protect the public as well as to improve the responsiveness of those involved in emergency management.

Restrictions on the distribution of foodstuffs, pre-defined by the European Commission (maximum permitted levels, MPLs), which would be enforced in the event of a new accident, are very low. For releases corresponding to the S3 source term, distribution could be prohibited at distances far away from the site of release (over 100 km) for periods of varying length depending on the radionuclides released (particularly iodine-131, which would practically disappear within a few months).

These observations led to a search for ways to significantly reduce 'maximum conceivable releases' for future reactor projects (see Section 17.10 below which discusses how core-melt accidents were handled in EPR design) and to reduce, as much as possible, potential release from operating reactors in the context of a continuous safety improvement approach.

Following the interministerial directive of 7 April 2005 on measures to be taken by public authorities regarding an event leading to a radiological emergency, ASN set up a Steering Committee for the Management of the Post-accident Phase of a Nuclear Accident or Radiological Emergency (*Comité directeur pour la gestion de la phase post-accidentelle d'un accident nucléaire ou d'une situation d'urgence radiologique*, CODIRPA), mentioned in Section 2.3, whose task is to define public policy on organizing action taken by public authorities under post-accident conditions. The policies formulated by this body in 2012[577] propose immediate actions (if substantiated) for the short-term post-accident phase as soon as the emergency phase is over, as well as the long-term post-accident phase, in order to:

- limit exposure of the public,
- reduce land contamination,
- prohibit the consumption and distribution of contaminated foodstuffs,
- manage contaminated food waste and other waste,
- monitor radiation levels in exposed populations.

In 2014, following the Fukushima Daiichi nuclear power plant accident, the French government published a national emergency response plan to be implemented in any major nuclear or radiological accident, which defines emergency response organization as well as the strategy to apply and the main measures to be taken by the government in terms of public health, environmental protection, continuity of social and economic activities, and international relations[578].

[577] Accessible at http://www.french-nuclear-safety.fr/Information/News-releases/National-doctrine-for-nuclear-post-accident-management (5 October 2012 report).

[578] Report 200/SGDSN/PSE/PSN, February 2014 edition, accessible at: https://solidarites-sante.gouv.fr/IMG/pdf/SGDSN_parties1et2_270114.pdf.

17.8. Ultimate emergency operating procedures

Similar to the H procedures, the initial letter and the numbering of the U ultimate emergency procedures were set during studies that followed the accident at Three Mile Island, before the logical coherence of the studies had been fully developed.

The U1 procedure is intended to prevent core degradation (or, if degradation occurs, to keep the core inside the vessel) using all available water injection systems. This procedure is mentioned in Chapter 33 on incident and accident operation and is clearly a preventive procedure for core melting, even though it is also for 'managing' this type of situation.

The U2 procedure, Action to Take in the Event of a Containment Isolation Fault, was presented above.

Although it is classified with the other emergency procedures, the U3 procedure, Use of Mobile Equipment to Back up Safety Injection and Spraying in the Containment, already mentioned in Section 13.2, does not correspond to containment protection after core melt. On the contrary, it is a preventive or mitigating measure with regard to this phenomenon.

As an extension of the H4 procedure, which plans for mutual backup of the stationary water-pumping equipment of the low-head safety injection system and of the containment water spray system, the U3 procedure takes into account total loss of pumping equipment. It essentially provides for the implementation of pumping equipment using pre-installed connection devices that are accessible after an accident and, if necessary, the implementation of an exchanger. This equipment is not installed in stationary locations at the units.

The U5 procedure, Containment Decompression, was presented above.

In parallel to the procedures used by operators, the nuclear safety engineer uses the continuous post-incident monitoring procedure (now referred to as 'continuous state monitoring'), then, after switching to the U1 procedure, the continuous emergency-state monitoring procedure. This subject is discussed in Chapter 33.

17.9. On-site emergency plan

The actions described above for a nuclear power plant are part of a broader plan consisting of principles that are common to all nuclear facilities, i.e. the 'on-site emergency plan'[579]. In particular, the plan defines relationships within EDF and those with outside responders (public authorities, including ASN and its technical support services [the weather service Météo France, IRSN, etc.]) whose response is organized by other plans presented in Chapter 38.

[579] *Plan d'urgence interne*, PUI.

The on-site emergency plan applies inside the nuclear site and is implemented under the operator's responsibility. It concerns:

- operating and safeguarding the facility,
- responding to any injuries on site,
- protecting site personnel,
- alerting and informing public authorities.

An on-site emergency plan may be initiated by the operator[580]:

- in non-radiological situations (fire, injury, etc.),
- in situations with confirmed radiological risk (risk of releasing radioactivity inside the facility or to the environment that could lead to exposing workers or nearby populations),
- in other situations, some of which do not involve nuclear safety (such as chemical contamination), where it may appear necessary to mobilize significant resources.

The local organization of EDF at a nuclear power reactor site where an accident has occurred is described in Chapter 38. EDF has several on-site emergency plans[581], including the following:

- Radiological Safety On-site Emergency Plan: covers situations for which facility safety is significantly affected or for which there is a risk of release of radioactive substances inside the facility or to the environment, that could cause exposure to people working outside the controlled area or to nearby populations. This on-site emergency plan covers the case of fire in a controlled area;
- the On-site Emergency Plan for Climatic and Similar Safety Hazards: covers all external climate hazards (such as floods or extreme cold or heat) and similar events (hydrocarbons, algae, and plant debris in pumping stations, etc.) that may affect several units at a site;
- the Toxic Hazards On-site Emergency Plan: concerns situations of gaseous release of hazardous products inside the facility (ammonia cloud from an effluent treatment station) or outside the facility (affecting an industrial site near a nuclear power plant or involving a traffic accident);
- the On-site Emergency Plan for Fire Outside Controlled Areas: pertains to fires within the basic nuclear installation perimeter, outside controlled areas;
- the Emergency Rescue On-site Emergency Plan: concerns situations where at least five people are seriously injured.

[580] These three types of situation correspond to three 'levels' of intervention defined in the on-site emergency plan, numbered 1, 2 and 3, respectively.

[581] *Mémento sûreté nucléaire en exploitation* (Memento on Operational Nuclear Safety), EDF, 2016.

The rest of this chapter mainly focuses on the first of these on-site emergency plans.

Article 2.3 of ASN decision 2017-DC-592 dated 13 June 2017 establishes the following requirements in terms of on-site emergency plan content: "The operator lays out the on-site emergency plan in an operational document including:

a) a map of the site, its activities, and its environment, showing the access routes to the facilities and the discharge stacks;

b) the criteria for initiating the on-site emergency plan, defined based on the conclusions of the design study for this plan [...]" (see Section 2.5) "and taking into account, as necessary, the operating procedures for incidents and accidents provided or called for in the general operating rules [...];

c) for informational purposes, a summary of the kinetics and consequences of accident scenarios used in defining the on-site emergency plan, described in the design study of this plan, included in the safety analysis report and, if applicable, requiring the implementation of the off-site emergency plan;

d) the description of the organization and equipment planned for managing emergency situations [...]. If necessary, the use of means under the responsibility of public services, public organizations or contractors is indicated;

e) the documentation specifically used by designated emergency team members, including:

   - a decision-making support document for initiating the on-site emergency plan and, if necessary, the identification of emergency situations that could lead the prefect to implement the off-site emergency plan [...];
   - operational sheets indicating, for each on-site emergency plan function, the actions to be taken, their timeline, and their exact phasing. Each sheet describes the main actions, referring as necessary to operating procedures in which the specific conditions and means are indicated;
   - message templates providing the information [...] to be transmitted [...];

f) the planned provisions for protecting people at the site not involved in managing the emergency situation [...]."

Since the 1980s, with regard to situations involving radiological risk, anticipatory studies by EDF and IRSN have focused on scenarios to prepare support material for rapidly making a first prognosis of the possible development of a real emergency situation and the associated consequences, as part of the 'diagnostics-prognostics' approach discussed in Section 38.7.1. These scenarios (commonly called 'standard accidents') correspond to accidents used for the deterministic studies in the safety analysis reports or to variants. In this type of study, the modified assumptions compared to those of the safety analysis reports may concern, for example, the type and number of aggravating failures considered or weather conditions.

17.10. Approach adopted for the EPR

As indicated in Chapter 18, ambitious safety targets have been set for the EPR since 1993. These targets aim in particular to significantly reduce radioactive releases that may result from all conceivable accident situations, including core-melt accidents. This has led designers to adopt the specific design provisions (briefly mentioned in Chapter 18) described below. The core-catcher, a new system engineered for EPRs, is an example of these provisions.

17.10.1. General safety objectives

General severe-accident safety objectives for the EPR were stipulated in Decree 2007-534 of 10 April 2007, which authorized creation of the 'Flamanville 3' basic nuclear installation, based on "Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors". They are noted below.

Core-melt accidents that could lead to significant early releases must be 'practically eliminated'. If they cannot be considered as physically impossible, design provisions must aim to exclude them. This applies in particular to accidents featuring high-pressure core melt.

Low-pressure core melt accidents must be dealt with so that the associated maximum conceivable releases would require only very limited protective measures for the public in terms of time and space. This implies:

- no permanent relocation of the population,
- no need for emergency evacuation beyond the immediate vicinity of the nuclear site,
- limited sheltering,
- no long-term restrictions on the consumption of foodstuffs.

As regards low-pressure core-melt accidents, given the wide range of possible accident conditions, compliance with this target must be assessed by evaluating the radiological consequences of various representative accidents that have been defined. This involves taking into account the detailed design of the facility.

17.10.2. 'Practical elimination' of core-melt conditions that could lead to significant early releases

In the 1990s, during French-German discussions on the safety of the next generation of pressurized water reactors (in practice, EPRs), the concept of 'practical elimination' was introduced with regard to certain core-melt situations. These situations are at least theoretically possible and could lead to 'significant early' releases for which realistic provisions significantly and demonstrably limiting the consequences do not appear to be possible. The technical guidelines mentioned above indicate that “the core-melt accidents that would lead to significant early releases shall be practically eliminated; if they cannot be considered physically impossible, measures [...] must be implemented to exclude them.” It was also recognized that ‘practical elimination’ could not be based on a probabilistic generic threshold.

Internationally, the INSAG-10 report, released in 1996, indicates that “for advanced designs, deterministic and probabilistic approaches must be used to demonstrate that hypothetical sequences of severe accidents leading to significant radioactive releases due to early containment failure are essentially eliminated with a high degree of confidence”. In 1999, the INSAG-12 report returned to this concept, making formal use of the expression ‘practical elimination’.

Without explicitly referring to the concept of ‘practical elimination’, Article 3.9 of the ‘INB Order’ of 7 February 2012 allows this type of approach, indicating that: “The demonstration of nuclear safety must prove that accidents that could lead to large releases of hazardous substances or to hazardous effects off the site that develop too rapidly to allow timely deployment of the necessary population protection measures are physically impossible or, if physical impossibility cannot be demonstrated, that the measures taken on or for the installation render such accidents extremely improbable with a high level of confidence.”

In January 2018, IRSN published on its Internet site a document in its ‘Safety Approaches’ collection[582], entitled The ‘Practical Elimination’ Approach of Accident Situations for Water-cooled Nuclear Power Reactors. The most noteworthy aspects are discussed below.

For pressurized water reactors, the ‘practical elimination’ approach is applied in situations characterized by a risk of rapid, high-energy physical phenomena that could lead to short-term containment failure and significant early releases. For these situations, the objective is to try to eliminate them; but the only way to solidly demonstrate that they have been eliminated is to show that they are physically impossible. If this is not the case, then the designer must show that ‘all’ necessary measures have been taken to make these situations extremely improbable with a high degree of confidence, i.e. they are ‘practically eliminated’.

Implementing a ‘practical elimination’ approach begins in the early design stage by identifying the situations in question, mainly based on an investigation of the possible failure modes of the containment or the containment ‘extension’ (concept explained in Section 6.3).

To ‘practically eliminate’ a situation thus identified, the first step consists in carefully examining the possibilities of making it physically impossible. If this turns out to be (reasonably) impossible, concrete measures must be defined and implemented to establish with a high degree of confidence that the situation is highly improbable.

[582] This document describes IRSN’s approach to ‘practical elimination’ and its place in the safety demonstration.

In a pressurized water reactor, these types of situation are varied (rapid and massive reactivity insertion accidents in the reactor core, overall hydrogen detonations and in-vessel and ex-vessel steam explosions that compromise containment integrity, containment bypass if a core-melt accident occurs, etc.). Whether they are 'practically eliminated' can only be assessed case by case, based on deterministic considerations, with probabilistic insights if necessary. This assessment is based on the physical characteristics of the facility and on the robustness and reliability of the provisions implemented to prevent the situation that is to be 'practically eliminated'. The chosen measures are subject to design, construction and operating requirements; hazards and aspects related to human factors must also be taken into account in the definition and design of these measures.

For the EPR, core-melt situations that must be 'practically eliminated' are as follows (see also the Focus feature in Section 18.2.2):

- high-pressure core-melt accidents that could lead to direct heating of containment gases or steam generator tube rupture,
- fast-reactivity insertion accidents, in particular those caused by rapid injection of insufficiently borated water in the reactor core,
- in-vessel and ex-vessel steam explosions and overall hydrogen detonations[583] that could compromise containment integrity,
- core-melt accidents with containment bypass (via the steam generators or the loops connected to the reactor coolant system).

▶ 'Practical elimination' of high-pressure core-melt situations

In order to avoid high-pressure vessel failure (pressure greater than an order of magnitude of 15-20 bars) or an induced steam generator tube rupture, the top of the EPR pressurizer is fitted with three pressure relief safety valves and other dedicated valves for cooling the reactor in the 'feed-and-bleed mode' or for emergency blowdown of the reactor coolant system (see Figure 17.4). The three pressure relief safety valves protect the reactor coolant system from overpressure. 'Feed-and-bleed' mode cooling is used in the event of total loss of the steam generator feedwater supply. Emergency blowdown of the reactor coolant system is used to prevent high-pressure core-melt. The three pressure relief safety valves and the dedicated 'feed-and-bleed' and emergency blowdown valves all discharge into the same letdown line, which carries the water, steam, or water/steam mixture to the pressurizer relief tank (PRT).

In addition, design provisions have been adopted to limit the diffusion of fragmented corium particles in the containment atmosphere in the event of vessel failure so as to avoid 'direct heating' of the containment gases. These design provisions apply to the reactor pit and its ventilation system and are intended to prevent large amounts

[583] Detonation is distinct from deflagration.

of corium leaving the reactor vessel from being carried from the reactor pit to the free volume of the containment.

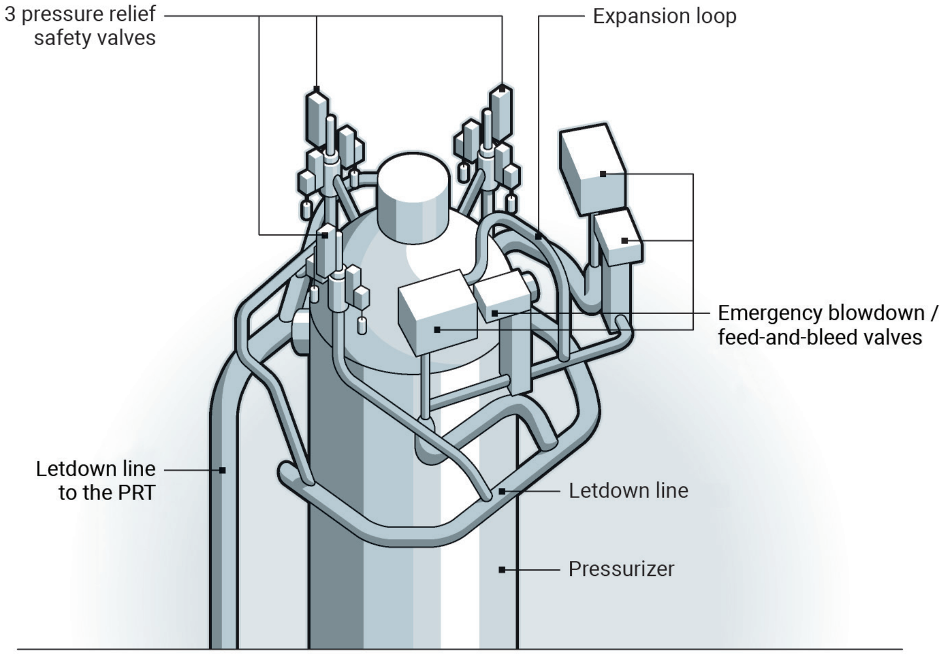

3 pressure relief safety valves
Expansion loop
Emergency blowdown / feed-and-bleed valves
Letdown line to the PRT
Letdown line
Pressurizer

Figure 17.4. Emergency blowdown of the EPR coolant system. Didier Jacquemain/IRSN Media Library.

▶ 'Practical elimination' of fast-reactivity insertion accidents

The 'practical elimination' of fast-reactivity insertion accidents by transfer of an insufficiently borated water 'plug' into the reactor core requires a detailed investigation of the various possible dilution scenarios that takes into account all prevention and protection provisions for each scenario.

The analysis follows the three steps recommended in the technical guidelines applicable to the EPR:

- definition of the maximum volume of a water plug without boron for which the subcriticality of the core has been demonstrated. This is based on neutron physics and thermal-hydraulic considerations pertaining to core subcriticality, independent of the anticipated dilution accident;
- definition of provisions to ensure that this maximum volume is not exceeded during any of the anticipated dilution accidents;
- conducting a probabilistic assessment to assesse the adequacy of the provisions implemented.

▶ 'Practical elimination' of the steam explosion risk

To prevent steam explosions in the event of high-temperature corium flows into the reactor pit, EPRs are designed with provisions making it impossible for water to enter the reactor pit before vessel failure occurs, even in the event of rupture of a reactor coolant system pipe.

EPRs also feature design provisions that avert steam explosions by preventing water from entering the spreading compartment of the core-catcher before the corium reaches it.

▶ 'Practical elimination' of the hydrogen detonation risk

The design pressure and temperature of the inner containment wall must ensure containment integrity even after an overall deflagration of the maximum amount of hydrogen that may be present in the containment during low-pressure core-melt accidents.

Moreover, the containment volume and the mitigation measures, such as passive catalytic recombiners, must be capable of reducing the hydrogen concentrations in the containment atmosphere to prevent the possibility of an overall hydrogen detonation.

Lastly, the containment internals must be designed to prevent the possibility of high local hydrogen concentrations, as far as reasonably possible. If it is not possible to demonstrate that the local hydrogen concentration remains below 10%, the absence of any deflagration-to-detonation transition and fast deflagration must be demonstrated. Otherwise, appropriate provisions must be implemented, such as reinforced walls on the corresponding compartments and the containment.

▶ 'Practical elimination' of core-melt situations with containment bypass

Concerning core-melt situations with a significant steam generator tube leak (up to multiple steam generator tube rupture), the following situations must be studied: single or multiple steam generator tube rupture with loss of systems required to mitigate the rupture, single or multiple steam generator tube rupture with closure failure on the corresponding main steam isolation valve, steam-line break with tube leakage from the associated steam generator, and spurious opening of a secondary safety valve with tube leakage from the associated steam generator. The scenarios leading to natural circulation through the reactor coolant loops and the steam generators must be studied with precision.

17.10.3. Provisions for low-pressure core melt

Design provisions have been adopted for low-pressure core-melt accidents in the EPR in order to comply with the general objectives defined above. The main provisions are as follows:

– A core-catcher (see Figure 17.5) at the bottom of the containment recovers and cools the corium after rupture of the vessel lower head and the 'fuse hatch' underneath (metal grid covered with a 'sacrificial' layer of concrete[584]), then allows the corium to flow through a discharge channel. This core-catcher is designed to protect the containment basemat from corium-concrete interaction. Corium is cooled by spreading it over a large surface area (170 m^2) in a zone called the 'spreading compartment'. Design provisions prevent water from any part of the containment from entering this compartment before the corium spreads along its surface. The spreading compartment is also lined with a sacrificial concrete layer. The sacrificial concrete lining the fuse hatch and spreading compartment is designed to obtain appropriate characteristics in the molten mixture. When the corium reaches the spreading compartment, this causes valves to open and water to flow by gravity from a 2000 m^3 water tank (IRWST)[585] inside the containment. Once in the spreading compartment, the corium is flooded with water from this tank and is thus cooled. In addition, thermal loads on the basemat are limited by a thick steel plate located under the layer of sacrificial concrete and cooled by cooling channels connected to the containment heat removal system. Measures are also taken to avoid a significant steam explosion. A stack leads the steam produced in the spreading compartment into the containment and limits overpressure in this compartment. After condensation, the water returns to the IRWST.

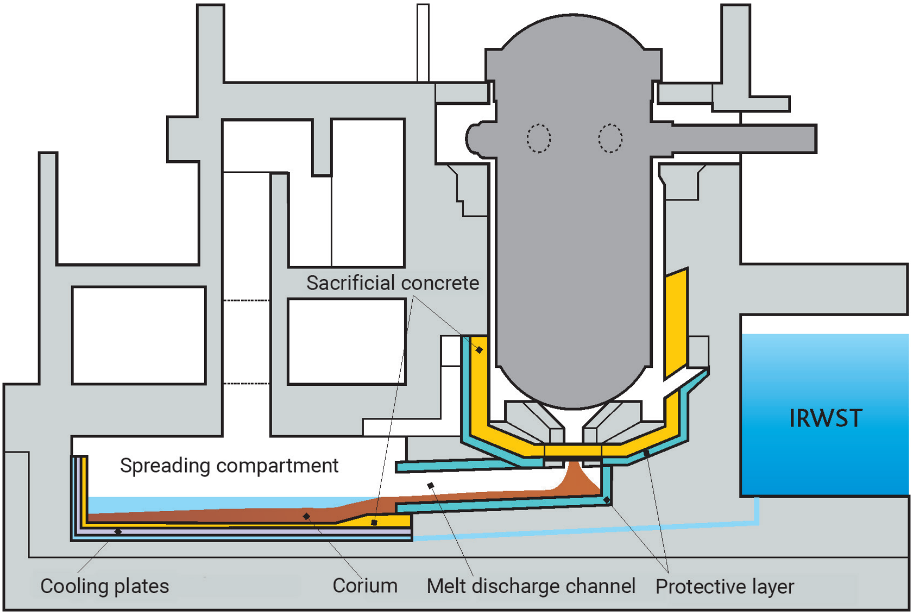


Figure 17.5. EPR core catcher. Georges Goué/IRSN Media Library.

[584] Concrete with a low melting point, unlike refractory concrete.
[585] In-Containment Refuelling Water Storage Tank, IRWST – see Chapter 18.

- the design pressure and temperature of the inner containment wall ensure containment integrity in the event of a severe accident:
  - for at least 12 h without removal of residual heat from the containment,
  - after an overall deflagration of the maximum amount of hydrogen that could be present in the containment;
- the containment heat removal system (CHRS) is used to control pressure inside the containment and preserve its long-term integrity in the event of a severe accident. This two-train system includes the IRWST tank, a heat exchanger with a specific intermediate system and a specific heat sink, as well as a containment spraying system. As mentioned above, this system may be used to cool corium in the catcher. Furthermore, the CHRS can be used to limit the production and release of volatile iodine in the reactor building by injecting sodium hydroxide in the IRWST;
- all the containment penetrations (including the equipment hatch[586]) open into buildings in which the atmosphere is ventilated and filtered. There must be no direct leakage path between the containment and the outside environment. Loops that may be used to carry radioactive substances outside the containment are contained inside peripheral buildings that feature appropriate confinement capability. Pressure-resistant penetrations in the containment must be designed to withstand loads resulting from core-melt accidents.

Qualifying the molten material catcher in accident conditions for core-melt situations has been mostly based on experimental programmes, such as the COMAS project (full-scale corium cooling tests performed by AREVA), the European CSC project (Corium Spreading and Coolability, qualification tests for the core-catcher design and the 'COMET design'[587] with reflooding from below), and the European ECOSTAR project (Ex-Vessel Core-Melt Stabilization Research, tests for the study of physical-chemical phenomena occurring during spreading and for the study of the efficiency of reflooding spread corium by adding water from above or below)[588].

[586] *Tampon d'accès des matériels*, TAM.

[587] From the name of the FzK facility in Germany in which this type of reflooding was tested.

[588] For more details, readers may consult Section 5.4.3.4 of Nuclear Power Reactor Core Melt Accidents – Current State of Knowledge, D. Jacquemain et al., Science and Technology Series, IRSN/EDP Sciences, 2013.

Chapter 18
New-Generation Reactors

An 'acceptable' level of safety is a notion that evolves over time, partly due to advances in knowledge, based on experience (in design and operation) and research and development work, and partly due to changes in the requirements applicable to operating nuclear facilities.

In many countries, the general public has lost confidence in the use of nuclear energy as a safe source for generating electricity, which has led to stopping new builds and phased decommissioning of reactors in service. In the USA in particular, this loss of confidence dates back to the time of the Three Mile Island accident. Since the Chernobyl accident, a similar trend has been seen in a number of other countries, especially European countries. Just as efforts to boost development in the nuclear power industry worldwide were underway, the accident at the Fukushima Daiichi nuclear power plant in Japan in March 2011 led some countries to announce that they would quickly be putting an end to their nuclear power programmes, while others decided not to pursue the development of nuclear power as an energy source (see Chapter 37).

In France, the first 900 MWe units built will have been in service for 40 years by around 2020 (i.e. the operating lifetime for which they were designed). In 2009, Électricité de France (EDF) announced its intention to extend the operating lifetime of its reactors beyond 40 years (EDF's 'DDF'[589] project), while also recommending the construction of new reactor units based on the project launched in the 1990s in conjunction with its German partners (the EPR project). In this regard, safety

[589] *Durée de fonctionnement* (operating lifetime).

organizations had already started to examine the safety objectives required for the next generation of pressurized water reactors in the late 1980s [590].

Design engineers, for their part, implemented similar approaches to develop the design basis for new build projects with significantly improved safety characteristics. Various types of reactor projects have therefore been developed by facility constructors, differing widely in technical terms, especially with regard to unit output and development time frames.

These projects can be divided into two main categories.

The first opted to develop designs based on existing reactor designs, incorporating experience feedback, studies carried out, including probabilistic studies, and advances resulting from research and development efforts. This approach takes full advantage of using proven technology, while introducing state-of-the-art innovation. This is known as 'evolutionary' design, as opposed to the second, more 'revolutionary' category of reactor design. Using technical solutions that are already well understood means that it is not necessary to build demonstration prototypes, as long as appropriate substantiation can be provided.

In the case of the second category, radically different solutions are sought; those who promote the development of such reactors focus on the more extensive use of 'passive' systems, i.e. systems that operate without requiring an external energy source.

This chapter does not set out to provide a comparative analysis of the different projects developed by reactor designers, but rather to show:

- the way in which France and Germany, in the 1990s, established new general safety objectives, including those applicable to the EPR project,
- the changes made to these general safety objectives applying to new reactor projects compared to those that had been established for the EPR project, including the integration of lessons learned from the Fukushima Daiichi nuclear power plant accident relative to extreme events,
- the way in which certain 'revolutionary' reactor designs deploy innovative systems to achieve these new general safety objectives.

[590] For more information, see article ref. BN3831 V1 in the magazine *Techniques de l'ingénieur* entitled *Approche de la sûreté des réacteurs nucléaires de generation III en France* (Safety Approach to Generation III Nuclear Reactors in France), by K. Herviou and J.-M. Évrard, 2012. Other types of nuclear power reactor, collectively known as GEN IV (or Generation IV) reactors, are not discussed in this chapter. For more information, see article ref. BN3832 V1 in the magazine *Techniques de l'ingénieur* entitled *Approche de la sûreté des réacteurs nucléaires de generation IV* (Safety Approach to Generation IV Nuclear Reactors) by J. Couturier (2013), or Overview of Generation IV (Gen IV) Reactor Designs/Safety and Radiological Protection Considerations, Reference Documents Series, IRSN, 2012.

18.1. Organization and framework of Franco-German discussions

This section gives a brief overview of the organization and framework of Franco-German discussions, which resulted in publication of the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors in 2000.

In 1989, the French and German constructors Framatome and Siemens set up a joint subsidiary, Nuclear Power International (NPI), to jointly develop products for export. It soon became apparent that it would be beneficial if these products could clearly be considered as approved by the French and German regulatory authorities.

As mentioned in Chapter 3, this industrial cooperation strengthened direct ties between the regulatory authorities in these two countries. For example, in 1990, a relatively small commission, the French-German Steering Committee (*Deutsche-Französischer Direktionsausschuss*, DFD), was created, whose members included the Director of France's Directorate for the Safety of Nuclear Installations (*Direction de la sûreté des installations nucléaires*, DSIN), and his German counterpart from the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (*Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit*, BMU), assisted by the Director of the French Institute for Protection and Nuclear Safety (*Institut de protection et de sûreté nucléaire*, IPSN) and the Society for Plant and Reactor Safety (*Gesellschaft für Anlagen-und Reaktorsicherheit*, GRS), the technical support branches of the French and German regulatory authorities, respectively.

In 1992, EDF, the German power utilities and Nuclear Power International (NPI) formed a partnership to develop a pressurized water reactor named the EPR (European Pressurized water Reactor), with construction of the first unit scheduled to start in 1998.

French and German regulatory authorities, for their part, had been reflecting for several years on nuclear power reactors of the future, based on a national approach. For example, in France, in May 1991, the Directorate for the Safety of Nuclear Installations (DSIN) sent out a letter, based on proposals made by IPSN, containing guidelines relative to desirable safety enhancements at nuclear power plants featuring future-generation pressurized water reactors. Defining a joint Franco-German project obviously required continuing these discussions and studies within a Franco-German framework.

At the end of 1992, the DFD therefore decided that the French and German regulatory authorities would make a joint statement regarding the major safety options required for future nuclear power reactors, based on common opinions set out by groups of experts from both countries (the Advisory Committee on Reactors [GPR] and the *Reaktorsicherheitskommission* [RSK]), which were based on studies jointly conducted by IPSN and the GRS. The DFD also decided that a common approach to safety with regard to future pressurized water reactors should be defined before industry submitted its main safety options for the EPR project. As a result, in June 1993, the French and German regulatory authorities published a document presenting this approach, drafted by the GPR and the RSK and based on proposals put forward by IPSN and GRS.

Discussions held between the French and German safety organizations soon led them to conclude that, to build new reactor units at the beginning of the 21st century, the way forward was to build 'evolutionary' reactors, derived from reactor designs already in service or under construction in France and Germany.

The Advisory Committee on Reactors, as requested by the French regulatory authority, prepared a document presenting the safety approach and the general safety requirements to be applied to the design and construction of a new series of new-generation pressurized water reactors. Entitled Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, the document was adopted in October 2000. These guidelines have served as a reference document for the EPR design.

The next section presents the main additions and changes made as compared to earlier reactor series (up to the N4 series).

18.2. Progression of safety objectives and design options for the EPR project

A number of safety-related changes adopted for the EPR project have been mentioned in previous chapters (for example, relating to core-melt accidents), and others will be covered in later chapters on operating safety, experience feedback from major accidents and emergency response management. Certain changes are mentioned again (sometimes in greater depth) in this section, in order to present a comprehensive view of their role in the EPR project.

18.2.1. General safety objectives

The accident at the Chernobyl nuclear power plant (see Chapter 34) clearly demonstrated the fact that significant releases of radioactivity into the environment entail not only the direct effects of ionizing radiation, but also cause wide-scale social and psychological disruption. It therefore appeared essential that new-generation reactors be designed in such a way as to prevent any release of radioactive substances liable to cause such disruption to the highest possible degree of confidence.

To this end, it was thought that a significant leap forward with regard to safety at the design stage was possible, as part of an evolutionary approach, taking on board the lessons learned from operating experience as well as probabilistic studies conducted with regard to existing reactor series and leveraging the results of research and development studies on safety – including studies on core-melt situations – with a view to obtaining a reduction in the calculated probabilities of accidents occurring and in the calculated releases of radioactive substances.

With this in mind, three key objectives were set out compared to earlier reactor designs:

- to reduce the number of incidents (meaning 'significant events' as defined in Section 21.3) with a view to reducing the likelihood of accident situations resulting from such events,
- to significantly reduce the probability of core melt.

  On this subject, the technical guidelines mentioned above stipulate that "implementation of improvements in the defence in depth [...] at such plants should lead to the achievement of a global frequency of core melt of less than 10^{-5} per plant operating year, uncertainties and all types of failures and hazards being taken into account." Taking into account all types of initiating events liable to result in a core melt was a totally new approach compared to earlier reactors;
- to significantly reduce the radioactive releases that could result from all conceivable accident scenarios, including accidents with core melt.

  On this subject, the technical guidelines stipulate that:

  - "for accident situations without core melt, there shall be no necessity of protective measures for people living in the vicinity of the damaged plant (no evacuation, no sheltering)";
  - "low pressure core-melt sequences have to be dealt with so that the associated maximum conceivable releases would necessitate only very limited protective measures in area and in time for the public. This would be expressed by no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in consumption of food."

  In addition: "Accident situations with core melt which would lead to large early releases have to be 'practically eliminated': if they cannot be considered as physically impossible, design provisions have to be taken to design them out. This objective applies notably to high-pressure core-melt sequences."

  The technical guidelines also stipulate that "decay heat must be removed from the containment building without venting device; for this function, a last-resort heat removal system must be installed."

In addition to the above, a fourth objective was added to the technical guidelines pertaining to radiological protection, namely to reduce individual and collective received doses for workers during normal operation and in the event of operating incidents. The guidelines state that, for "normal operation and abnormal occurrences, one objective is the reduction of individual and collective doses for the workers, which are largely linked to maintenance and in-service inspection activities. Reduction of the occupational exposures shall be aimed at by an optimization process taking into account the data obtained from operating experience."

18.2.2. Events to be taken into account at the design stage and in deterministic and probabilistic analyses

As in the case of reactors in operation, the safety demonstration is based on a deterministic approach, supported by probabilistic studies and appropriate research and development work.

On this point, the technical guidelines specify that, for the purposes of the safety demonstration, "single initiating events have to be 'excluded' or 'dealt with' – that is to say that their consequences are examined in a deterministic way. Single initiating events can be 'excluded' only if sufficient design and operation provisions are taken so that it can be clearly demonstrated that it is possible to 'practically eliminate' this type of accident situations; for example, the reactor pressure vessel rupture and other large components (as steam generator secondary side or pressurizer) rupture can be examined in that way."

The technical guidelines stress the importance, for new nuclear power reactors, of reinforcing the defence in depth compared to existing reactors, including "a more extensive consideration of the possibilities of multiple failures and the use of diversified means to fulfil the three basic safety functions" (…), and to aim for a "substantial improvement of the confinement function, considering in particular the different possible failures of this function for core-melt situations." On this point, the guidelines emphasize the importance of 'detailed investigations' into certain specific multiple failure sequences, including "the total loss of the spent fuel cooling system, for which ambient conditions in the corresponding building and their impact on the structures and systems located in this building, as well as the possibilities to provide a water makeup or to repair the faulted components have to be completely assessed. Additional measures have to be implemented as far as necessary notably regarding support systems."

It should be remembered that, as mentioned in Chapter 17, the technical guidelines note that "the practical elimination of accident situations which could lead to large early releases is a matter of judgement and each type of sequence has to be assessed separately. Their 'practical elimination' can be demonstrated by deterministic and/or probabilistic considerations, taking into account the uncertainties due to the limited knowledge on some physical phenomena. It is stressed that 'practical elimination' cannot be demonstrated by compliance with a [generic] 'cut-off' probabilistic value."

The concept of 'practical elimination' then required some clarification when it was time for implementation, in order to specify, first, the characteristics of sequences to which the concept applies, and second, the specific requirements that should be applied to certain measures when applying this concept; this is explained in more detail in Section 17.10.2.

In addition to single initiating events (relevant to equipment and equipment operation) or events involving multiple failures, the safety demonstration must include an assessment of internal and external hazards, which can be supported by probabilistic assessments.

Causal relationships between internal and external hazards and individual initiating events must also be taken into consideration.

In addition to the ‘load case’ approach, the consequences of certain external hazards (such as earthquakes) at the facility need to be studied since some of them may constitute initiating events (for example, when non-safety-grade equipment becomes a hazard to safety-grade equipment). It is also important to characterize the intensity of external hazards for which a cliff-edge effect could occur; with regard to this point, including in the case of earthquakes, the technical guidelines state: “The designer has also to specify how he intends to prove the existence of sufficient design margins consistently with the general safety objectives [...] The margin assessment has to be achieved with the aim to demonstrate that no cliff-edge effect in terms of radiological consequences would occur for acceleration values postulated beyond the site-specific acceleration values; the corresponding methodology has to take into account the actual behaviour of representative equipment and the possibilities of simultaneous failures of equipment.”

Regarding probabilistic studies, the technical guidelines stress the importance of taking into account all reactor states during which events may occur (reactor-at-power states, intermediate states, shutdown situations – including when the reactor containment is open –, etc.), together with situations that could affect the fuel assembly cooling function in the spent fuel pool.

The technical guidelines recommend conducting a probabilistic safety assessment from the design stage and including at least internal events, in such a way as to obtain an initial assessment of the probability of core melt, with a survey of the possible consequences of various types of core damage situations on the confinement function, together with an assessment of the relative importance of accident sequences and common-cause failures.

Measures designed to prevent and mitigate the consequences of incidents and accidents must be deployed at different levels of defence in depth to ensure that facility safety does not depend on just one level. Furthermore, these measures can be diversified to mitigate any risk of common-cause failure. To this end, together with the deterministic approach, probabilistic safety studies should be developed and used from the reactor design stage and, subsequently, in more precise detail, to support engineering studies – when more precise information regarding the design becomes available. Probabilistic safety studies are used to help choose between several possible options, as well as to assess facility robustness and identify potential weaknesses. In particular, they are used to draw up the list of operating conditions with multiple failures that must be assessed as part of the safety demonstration for the plant, and to adequately characterize the measures designed to ‘practically eliminate’ certain situations.

Regarding external hazards, probabilistic safety studies may be used to assess facility performance in relation to more severe hazards than those used to design structures, systems and components and for combinations of hazards, including where these affect an entire site.

#FOCUS

Situations in which ‘practical elimination’ must be implemented

Various situations for which a ‘practical elimination’ approach must be taken are listed in the Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors:

- rapid injection of cold or insufficiently borated water in the reactor core;
- high-pressure core-melt situations (including the case of total loss of feedwater supply to the steam generators with failure of core cooling using the ‘feed-and-bleed’ mode);
- core-melt situations leading to in-vessel and ex-vessel steam explosions and general hydrogen detonations that could endanger containment integrity;
- bypassing the containment during a core-melt accident: here, the technical guidelines state that: “Accident sequences involving containment bypassing (via the steam generators or via circuits connected to the primary system which exit the containment) have to be ‘practically eliminated’ by design provisions (such as adequate piping design pressure) and operating provisions, aimed at ensuring reliable isolation and also preventing failures”;
- fuel melt in the spent fuel pool; measures must be taken to manage total loss of the spent fuel pool cooling system while maintaining the confinement function; otherwise, the probability of water boiling in the spent fuel pool must be reduced by means of adequate improvements, including support systems for the pool cooling system.

The general safety objectives and the design options implemented for the spent fuel pool are described in Section 15.5.

18.2.3. Main provisions for preventing incidents and accidents

Without going into the finer details of the safety organizations’ analysis of the EPR project, this section describes, for the purposes of illustration, certain features of the Flamanville 3 EPR in order to highlight the main new characteristics regarding safety options and design choices in comparison to earlier reactors.

The Flamanville 3 EPR is a four-loop pressurized water reactor with a high power rating of 1675 MWe[591], housed in a double-wall containment with a leaktight liner on

[591] French Decree 2007-534 of 10 April 2007 granting the construction authorization for the Flamanville 3 EPR sets the reactor’s thermal output at 4500 MW.

the intrados of the inner containment wall, a leak recovery system between the two containment walls and filtration of leakage before it is released via the stack.

The containment is designed for the bounding accident conditions defined in the reference operating conditions (also known as Plant Condition Categories, or PCC – see definitions in the Focus feature in Section 8.1), operating conditions with multiple failures (RRC-A) and core-melt accidents (RRC-B).

The type of fuel used is the same as that used in earlier reactors; there are more fuel assemblies, making it possible to reduce mean linear power density[592] and achieve nominal operating margins, resulting in increased operational flexibility.

Incident and accident prevention, including prevention of core-melt situations, is based on reinforced redundancy for the main safety systems[593], diversifying the equipment used for certain systems and functions, and adequate physical or geographic separation between 'safety divisions'.

In addition, no action by the operators in the control room is required within the first 30 min following the onset of an incident or accident situation. No local action is required within the first hour. No additional heavy equipment needs to be brought to the site within the first three days.

The main safety systems are therefore made up of a number of trains located in different buildings and supplied by different 'electrical divisions' (see Figure 18.1).

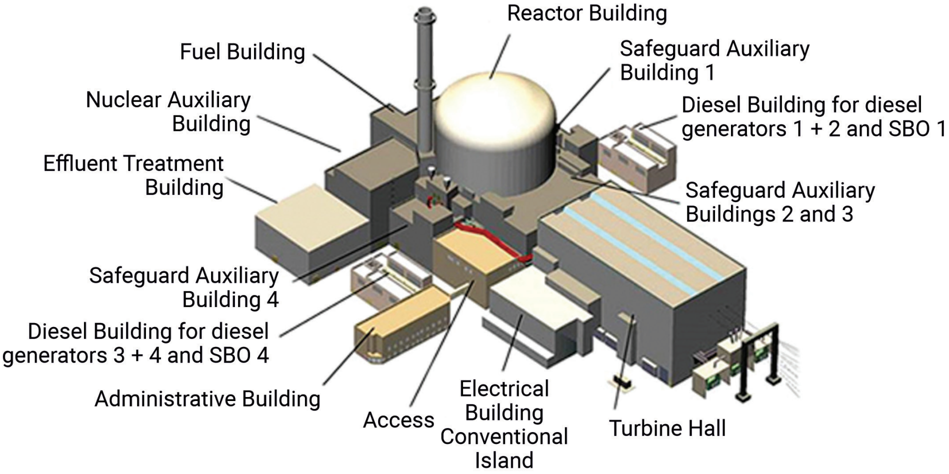

Reactor Building
Fuel Building
Safeguard Auxiliary Building 1
Nuclear Auxiliary Building
Diesel Building for diesel generators 1 + 2 and SBO 1
Effluent Treatment Building
Safeguard Auxiliary Buildings 2 and 3
Safeguard Auxiliary Building 4
Diesel Building for diesel generators 3 + 4 and SBO 4
Administrative Building
Electrical Building Conventional Island
Access
Turbine Hall

Figure 18.1. Layout of the main Flamanville 3 EPR buildings. IRSN.

[592] Namely, 155 W/cm in the case of the Flamanville 3 EPR, compared to 180 W/cm in the case of N4 reactor units.

[593] This is also related to certain choices pertaining to in-service maintenance, i.e. maintenance conducted with the reactor in operation.

Thus, as noted in Section 7.2, the safety injection system used, for instance, in the event of a break in the main primary system, includes four trains, each of which is capable of ensuring the safety functions for which the system is designed.

The 'medium-head' safety injection system pump discharge pressure is designed to prevent water discharge through the secondary system discharge valves in the event of steam generator tube rupture.

The low-head safety injection system is equipped with heat exchangers designed to remove decay heat in the cases considered in the reference operating conditions (PCC). The containment spray system installed in earlier French reactor units is therefore no longer required.

Depending on the line-up, the low-head safety injection system may take on the role of decay heat removal system (unlike earlier reactors). This design makes it necessary to circulate the water from the reactor coolant system outside the reactor containment when the reactor is shut down, and thus requires careful attention to limit the risks of containment bypass.

An emergency boration system[594] consists of two redundant trains.

In accordance with the technical guidelines, a containment heat removal system consisting of two trains[595] is available for use in core-melt situations. Heat is removed and sent outside the reactor containment by a cooling system that is different from those associated to the engineered safety systems. This design requires the 'practical elimination' of any severe accident situations that could lead to containment bypass.

The emergency feedwater system for the steam generators used to cool the reactor in the event of certain incident or accident situations consists of four trains (4 x 50%) each feeding one of the steam generators[596]. Unlike earlier French reactor units, this system is not used during startup and shutdown sequences, for which a specific system is used.

The power supply to the 'electrical divisions' that supply the power required to operate the different safety system trains is backed up by four main diesel generators used in the event of loss of off-site power supply from the national grid.

[594] For 900 MWe, 1300 MWe and 1450 MWe reactors, emergency boration entails injecting highly concentrated borated water via the safety injection system in the case of 900 MWe series reactors (by means of a very high-concentration boron cartridge used in association with the high-head injection system), or via the chemical and volume control system in the case of 1300 MWe and 1450 MWe reactors.

[595] Beyond 15 days after the onset of a core-melt accident, one train is enough to remove decay heat.

[596] In the case of certain accident sequences, taking into account the possibility that one train may be lost as an aggravating event and another may be unavailable due to maintenance operations, the line-up of headers before and after the system pumps is designed to ensure adequate water supply to the steam generators to remove decay heat.

Two station blackout diesel generators, diversified[597] with respect to the main generators, supply power to equipment required to manage a situation involving total loss of electrical power (off-site power failure combined with main generator failure) and to equipment used in managing core-melt accidents.

Last, batteries providing 24-h autonomy can be used to supply essential equipment needed for the short-term management of a total loss of power (off-site supply and main generators and station blackout generators) leading to core melting.

As per the technical guidelines, the design pressure and design temperature of the inner containment wall are calculated to allow for a grace period of at least 12 h without removal of decay heat from the containment following a severe accident, while containment integrity/leaktightness are ensured even in the case of a overall deflagration of the maximum amount of hydrogen that could be present in the containment building during low-pressure core-melt accidents.

The containment, the fuel building and two of the safeguard buildings (buildings housing the 'engineered safety systems') are protected against aeroplane crashes (see Figure 18.2). This protection is provided by the outer reactor containment[598], a thick concrete structure, which has been extended (by way of the aeroplane crash [APC] shell) to cover the fuel building and two safeguard buildings. Inner walls, separated from the protective wall of these buildings, are provided to mitigate the shock caused by an aeroplane crash or explosion, preventing propagation to structures, systems and components.

The goal of the design and manufacture of the main primary system and the main secondary system was to ensure that they would be resistant to ageing, achieve a very high level of quality and be capable of passing demanding inspections to ensure that the requirement of excluding main system pipe breaks could be met[599]; the aim of this was to exclude the mechanical effects of complete double-ended guillotine breaks – including on the reactor vessel internals – thereby eliminating the need to deploy pipe-whip restraints. The safety injection system and the containment are, nonetheless, still designed to withstand instantaneous double-ended guillotine breaks in these lines (although not under PCC conditions).

[597] Diversification includes contracting with different suppliers along with a certain number of technical characteristics.

[598] Nonetheless, the APC shell is not subject to a (static) confinement requirement in the event of radioactive release outside the (inner) reactor containment or outside the fuel storage building. For the Flamanville 3 EPR, the Containment Annulus Ventilation System ensures dynamic confinement.

[599] Including the use of austenitic steels and fabrication by forging, the absence or reduced use of longitudinal welds in favour of circumferential welds, and allowing the use of two inspection methods for dissimilar welds, etc.

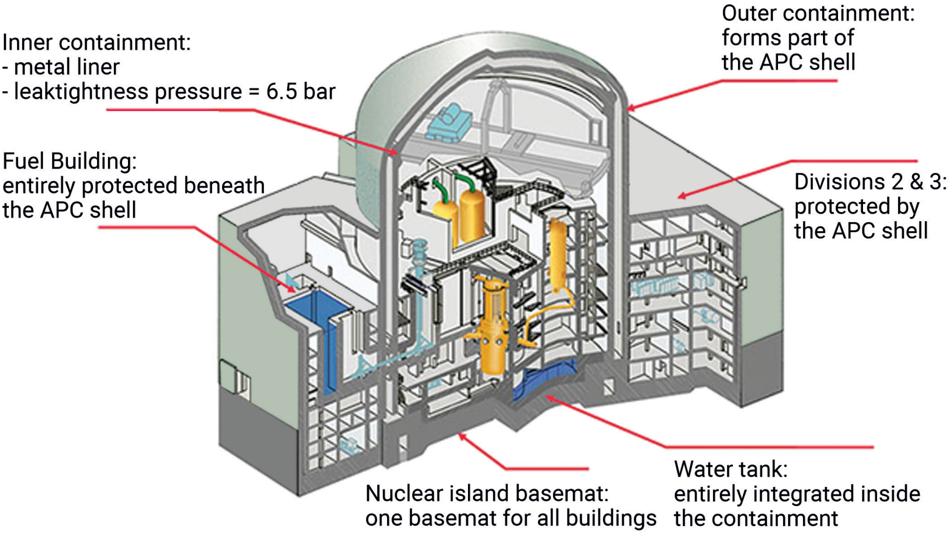

Inner containment:
- metal liner
- leaktightness pressure = 6.5 bar
Outer containment: forms part of the APC shell
Fuel Building: entirely protected beneath the APC shell
Divisions 2 & 3: protected by the APC shell
Water tank: entirely integrated inside the containment
Nuclear island basemat: one basemat for all buildings

Figure 18.2. Section view of EPR including the APC shell. IRSN.

In accordance with the French Pressure Equipment Order, the main primary system pipes and some main secondary system steam pipes are classified at the highest safety level, N1.

The (borated) water tank for the safety injection system[600] is located inside the reactor containment and is called the In-Containment Refuelling Water System Tank (IRWST), with a capacity of 2000 m^3. This is a significant simplification: if a safety injection is performed, there is no longer any distinction between the direct injection phase during which the water injected in the reactor core comes from an external tank, as in the case of earlier reactor series (using the spent fuel pool cooling system), and the recirculation phase in which the water comes from the sumps in the containment building. This means that there is no longer any need to make changes to the valve configuration.

The standard earthquake design basis for buildings in the nuclear island and for equipment important to safety has a more stringent floor response spectrum[601] than that applied to reactors currently in operation. Furthermore, the buildings in the nuclear island are built on a single basemat, ensuring improved overall performance in the event of an earthquake.

[600] Borated water tank, supplying the safety injection system and the containment heat removal system. The water held in the IRWST is also used to fill the reactor cavity when loading and unloading fuel in the reactor.

[601] Response spectrum, in terms of acceleration, of oscillators functioning at different specific frequencies.

The platform elevation for the entire Flamanville site (+ 12.40 m NGFN[602]) ensures significant margins in relation to the different possible flooding scenarios[603]. In addition, the external flood protection approach implemented for the EPR largely incorporates lessons learned from the partial flooding of the Blayais site on 27 December 1999, including the implementation of a protection area designed to protect the equipment required to reach and maintain a safe state in the event that the site is flooded.

18.2.4. Functional redundancy, independence between systems, system reliability

For the Flamanville 3 EPR, functional redundancy has been adopted to ensure different safety functions, in particular for cooling the fuel even in very degraded conditions.

In the event of a small break that causes the pressure in the reactor coolant system (RCS) to drop to the pressure of the secondary system, the fuel can be cooled by the secondary system to reach the medium-head safety injection system pump discharge pressure.

To ensure the reliability of core cooling by recirculating water using the safety injection system, which draws water directly from the sumps, a special arrangement was adopted for filtering out any debris produced by a break in the RCS, consisting of two[604] screening systems installed in series across the path of the debris:

- basket strainers at the edge of the internal reactor water storage tank (IRWST) described above, at the floor openings in large components,
- strainers in the middle section of the IRWST, where the suction lines leading to the pumps are installed.

Unlike previous reactors[605], the EPR also has a second heat sink, which can draw water from the intake channel or from the coolant water discharge pond (Ultimate Cooling Water System), which makes it less vulnerable to loss of the main heat sink.

The instrumentation and control system in the EPR relies on two ‘platforms’:

- the first platform (Teleperm XS) has been specifically developed for the nuclear industry and is dedicated to functions that protect the reactor in the event of incident and accident situations;

[602] *Nivellement général de la France normal* – French normal general datum system.

[603] See document on the ASN website published by Électricité de France entitled Complementary Safety Assessments of Nuclear Facilities Following the Fukushima Accident, 15 September 2011. The recommendations made in the ASN Guide No. 13: Protection of Basic Nuclear Installations against External Flooding (pending publication at that time) were taken into account.

[604] In addition to debris screens installed on the floor of large components.

[605] Work is planned to also provide reactors already in operation with a second heat sink, as part of the measures implemented as a result of lessons learned from the Fukushima Daiichi nuclear power plant accident (see Section 36.6.7).

– the second platform (SPPA T2000) was developed for the conventional power industry[606] and is used not only to ensure functions relating to normal operation, but also for certain functions that protect the reactor as part of the diversification of some of the functions performed by the Teleperm XS platform for controlling the reactor during incident and accident situations.

This architecture has raised several issues regarding how robust, or even acceptable, it is in terms of safety. EDF was able to provide adequate substantiation to justify its use. Meanwhile, EDF nonetheless implemented a change designed to improve the reliability of the protection functions that use the 'conventional industry' platform: this change entailed duplicating certain protection functions performed by the SPPA T2000 platform on the Teleperm XS platform, thereby making the I&C system more robust in the event of failure on the SPPA-T2000 platform combined with certain incident or accident situations.

18.2.5. Confinement preservation

In keeping with the general safety objectives adopted for the next generation of pressurized water reactors in the technical guidelines mentioned previously, the EPR presents a significant improvement to the confinement function, primarily by taking core-melt situations into account from the design stage. The related measures are described in more detail in Section 17.10.2 and are summarized below.

The free volume of the internal containment is very large, approximately 90,000 m^3. It is designed to withstand the overpressure produced by deflagration of the maximum amount of hydrogen that could be present in the internal containment during a core-melt sequence. Bearing in mind the presence of recombiners, designed to reduce the concentrations of hydrogen, this amount of hydrogen corresponds to 50% of the quantity produced by the reaction between all the cladding and the water vapour. The corresponding pressure is 6.5 bars absolute, which is higher than the pressure resulting from the complete break of a main primary system pipe.

The containment heat removal system designed for core-melt situations (as mentioned in Section 17.10.3) is made up of two trains; it uses a water spray system inside the containment to cool the containment atmosphere and control internal pressure. There is no emergency venting system in the containment.

In addition, as described in Chapter 17, to prevent core melt under pressure, the top of the EPR pressurizer is equipped with two parallel lines, each featuring two valves, the first for cooling in 'feed-and-bleed' mode and the second for emergency blowdown of the RCS.

[606] The SPPA T2000 platform uses various industrial and commercial software packages, with extensive use of bidirectional communication across networks that exchange information with each other and with equipment items belonging to different safety classes and different levels of defence in depth.

There are also provisions designed to prevent the basemat from being pierced by corium. In particular, a core-catcher located at the bottom of the containment serves to collect and cool corium after vessel lower-head melt-through, and a 'fuse hatch' below that, diverting the corium flow through a discharge channel. Once it has expanded throughout the core-catcher, the corium is cooled by water from the IRWST. The core-catcher and its operating principles are described in detail in Section 17.10.3.

It should be noted that many of the systems described for the EPR can be found in other power reactor designs, including ATMEA1, the 1100 MWe pressurized water reactor project jointly developed by Mitsubishi Heavy Industries and Framatome. Examples include the location of the in-containment safety injection water tank and the use of systems designed to prevent corium from penetrating the basemat.

18.2.6. Radiological protection

Two design choices regarding radiological protection for the EPR should be noted.

First, the materials used are chosen specifically to reduce activation of the structures and, consequently, to reduce the doses received by personnel during in-service inspection (for example, steels with low cobalt content used in the RCS, optimizing [reducing] the use of Stellite coatings for reactor vessel internal structures and valves[607], etc.).

A 'two-room' design has also been implemented for the Flamanville 3 EPR so that personnel can work inside the reactor building at times other than during unit outages, including to prepare for unit outage (seven days prior to shutdown and three days after restart). To reduce radiological exposure of personnel as much as possible, the reactor building is divided into an 'equipment compartment' (made up of the main parts of the RCS) and a 'service area' equipped with specially-designed bioshielding, where the atmosphere is compatible with the presence of people during operation.

18.2.7. Incorporating lessons learned from the Fukushima Daiichi nuclear power plant accident

The EPR was designed to meet the safety objectives stipulated in the technical guidelines written in the 1990s. The Fukushima Daiichi accident raised questions about facility robustness in terms of the ability to withstand extreme hazards.

In Europe, stress tests were carried out on existing reactors still in operation. In France these tests are referred to as the Complementary Safety Assessments (CSAs). Among other objectives, these complementary safety assessments were carried out to assess, for each facility in question, "the robustness of the facility beyond its design basis, by identifying, on one hand, any situations that could lead to a rapid degradation

[607] Stelitte is the name of a range of chrome and cobalt alloys designed for wear-resistance.

of the accident (i.e. a cliff-edge effect) and, on the other, measures taken to avoid these situations."[608]

Without going into too much detail regarding the CSAs, described further in Chapter 36 – and especially in Section 36.6.4 dedicated to the measures implemented as a result, not only for the French fleet of units in service but also in the case of the Flamanville 3 EPR under construction, and in Section 15.5 relative to spent fuel pools – some of the key points are discussed here.

As seen above, the EPR has taken advantage of being able to incorporate certain measures from the design stage (in comparison to reactors already in operation), which aim to prevent situations involving total loss of heat sinks and electrical power supplies, and to mitigate the consequences of a core-melt accident. The Flamanville 3 EPR also features better protection from external hazards such as earthquakes and flooding, and will benefit from a number of measures adopted by EDF following the Fukushima Daiichi nuclear power plant accident.

To begin with, one of the measures adopted by EDF following this accident entailed setting up a Nuclear Rapid Response Force (FARN) to assist any site in the French nuclear power plant fleet trying to manage a severe accident situation; the FARN can be deployed to a site within 24 h, with a first team on site within 12 h. The FARN is presented in Section 36.6.6.

In addition, the concept of a 'hardened safety core' has been implemented for the Flamanville 3 EPR. This is designed to provide not only equipment, but also the human and organizational resources necessary to keep under control, at least during the first few days after an accident (and until the FARN comes), the vital safety functions of the reactor in the event of total loss of heat sink or electrical power, including in the case of an extreme external hazard (that could affect the entire site). These resources must serve to:

- "prevent a fuel-melt accident or limit its progress,
- reduce or mitigate massive radioactive release,
- enable the licensee to fulfil its emergency management duties."[609]

For the Flamanville 3 EPR, various systems and equipment (new or already planned) were thus adopted to form this hardened safety core, including – to name only those specific to the EPR as mentioned above – the core-catcher to collect molten materials and the RCS blowdown lines (designed to stop core-melt accidents with pressure build-up).

Nonetheless, in line with ASN Guide No. 22, relevant to the design of new-generation pressurized water reactors (including reactors other than the EPR, which is already under construction), a new approach has replaced the concept of 'hardened safety core'. Based on the notion of 'design extension conditions', it incorporates external hazards of a much greater scale than those considered in design-basis scenarios.

[608] Request made to ASN by the French prime minister on 5 May 2011.
[609] As per the requirements issued in ASN decisions dated 26 June 2012.

18.3. International context: general safety objectives for new-generation reactors

At international level, discussions were initiated in the mid-1990s on what the general safety objectives should be for future power reactors. Of particular interest, in 1999, the INSAG[610] published INSAG-12, a revision of Safety Series No. 75-INSAG-3 published in 1988. This revision incorporates a number of changes to the document published in 1988 and emphasizes the need to focus attention, from the power reactor design stage, on preventing and mitigating the consequences of multiple-failure situations and accidents that could cause severe core damage, with a view to preventing containment failure in particular.

INSAG-12 states that for existing reactors (that existed at that time), the measures implemented should provide a frequency of occurrence of severe core damage of about 10^{-4} events per facility operating year, while implementation of accident management and mitigation measures could reduce by a factor of at least 10 the probability of large off-site releases requiring a short-term response. INSAG-12 considers that by applying the report's safety principles and objectives to future reactors, it would be possible to achieve a probability of severe core damage of approximately 10^{-5} per year per reactor. Another objective for these future reactors is the practical elimination of accident sequences that could lead to large early releases of radioactive substances.

Since the 2000s, a great deal of effort has gone into harmonizing safety objectives, resulting in the publication of new (European and international) documents. For example, texts based on the work conducted by WENRA, the International Atomic Energy Agency and for European Directive 2014/87/Euratom today form a set of reference documents that provide a consistent set of general safety objectives for the next generation of nuclear reactors in Europe.

In 2010, WENRA published[611] a position document setting out seven objectives for new reactors, covering the following subjects:

- normal operation, abnormal events and prevention of accidents,
- accidents without core melt,
- accidents with core melt,
- increased independence between all levels of defence in depth,
- safety and security interfaces,
- radiation protection and waste management,
- management of safety.

[610] International Nuclear Safety Group, see Chapter 3.

[611] WENRA Statement on Safety Objectives for New Nuclear Power Plants, November 2010.

In 2013, WENRA integrated the lessons learned in the wake of the Fukushima Daiichi accident in a new report[612], including the following objectives:

- reinforce facility robustness to withstand 'beyond-design-basis' external hazards,
- reinforce robustness to withstand situations involving total loss of heat sinks or electrical power supplies,
- improve response to situations impacting different units at the same site and/or the spent fuel pools,
- increase independence between the different levels of defence in depth, especially between Levels 3 and 4,
- improve long-term management of core-melt accident situations.

Most of the lessons learned can be found elsewhere, including in the revised 2014/87/Euratom version of Directive 2009/71/Euratom, and in the 2016 revision of the IAEA guide on Safety by Design.

The 2014 revision of the Directive sets a safety objective for nuclear facilities, taking up that adopted in the technical guidelines written in the 1990s for the next generation of pressurized water reactors, which is "to prevent:

- early radioactive releases that would require off-site emergency measures but with insufficient time to implement them,
- large radioactive releases that would require protective measures that could not be limited in area or time".

This revised version of the Directive specifies that Member States shall ensure that the national framework requires that the objective set out above:

- "applies to nuclear installations for which a construction licence is granted for the first time after 14 August 2014,
- is used as a reference for the timely implementation of reasonably practicable safety improvements to existing nuclear installations, including in the framework of the periodic safety reviews [...]"[613].

In France, all these studies led to the 2017 publication of ASN Guide No. 22 (available only in French to date) on pressurized water reactor design, drawn up jointly by IRSN and ASN, presented previously in Section 6.1. In particular, this guide includes a chapter on general safety objectives, taking into consideration the objectives adopted

[612] WENRA Report on Safety of New NPP designs –Study by Reactor Harmonization Working Group RHWG, March 2013.

[613] In Chapter 30, on periodic reviews, it is specified that this objective has been adopted as a reference for reassessments associated with the fourth ten-yearly outage for the French fleet of 900 MWe units, in connection with the plan to extend the operating lifetime of these reactors.

by WENRA in 2010, the requirements set out in the SSR-2/1 document published by the IAEA, and European Directive 2014/87/EURATOM.

While ASN Guide No. 22 only makes recommendations, it will be used as a reference for the design of new pressurized water reactors in France, just as the Technical Guidelines were used in designing the EPR.

18.4. Concepts highlighted in new reactor designs

The designers of new-generation reactors are developing many innovative systems. Some examples are discussed below:

- passive safety systems that make use of gravity for the AP1000,
- the SPOT system for the VVER-1200,
- the multi-group technology used for the NM EPR,
- the accumulators for the ATMEA1 reactor,

the common pool for modular NuScale reactors.

18.4.1. AP1000: gravity systems

The AP1000 is a pressurized water reactor with a power rating of approximatively 1150 MWe, developed by Westinghouse Electric Corporation (taken over by the Japanese firm Toshiba in 2006). Three AP1000 reactors have been built in China and were commissioned in 2018. AP1000 reactor safety is based on a number of passive systems, which eliminates reliance on an electrical power supply for at least 72 h.

The AP1000 has a number of innovative cooling systems, two of which are described below: a borated water gravity injection line, and a passive system for cooling the (metal) containment vessel in the reactor building[614].

The AP1000 has an IRWST tank (like the EPR), located outside the containment at a higher level than the reactor vessel (see Figure 18.3). This tank, filled with borated water, is kept at ambient temperature and pressure and is isolated from the RCS under normal operating conditions. One function of the IRWST is to supply makeup borated water to the RCS in the event of a loss-of-coolant accident. During this type of accident sequence, RCS pressure drops to a level low enough for the borated water in the IRWST to flow into the RCS by the force of gravity. Recirculation between the tank and the reactor is then actuated.

The containment is designed so that part of the water lost through the break is returned to the IRSWT, and the whole system is designed so that sufficient water is injected into the RCS to prevent core uncovery before and after recirculation is actuated.

[614] This containment vessel is encased inside a concrete structure, with the upper part of the containment open to the outside environment.

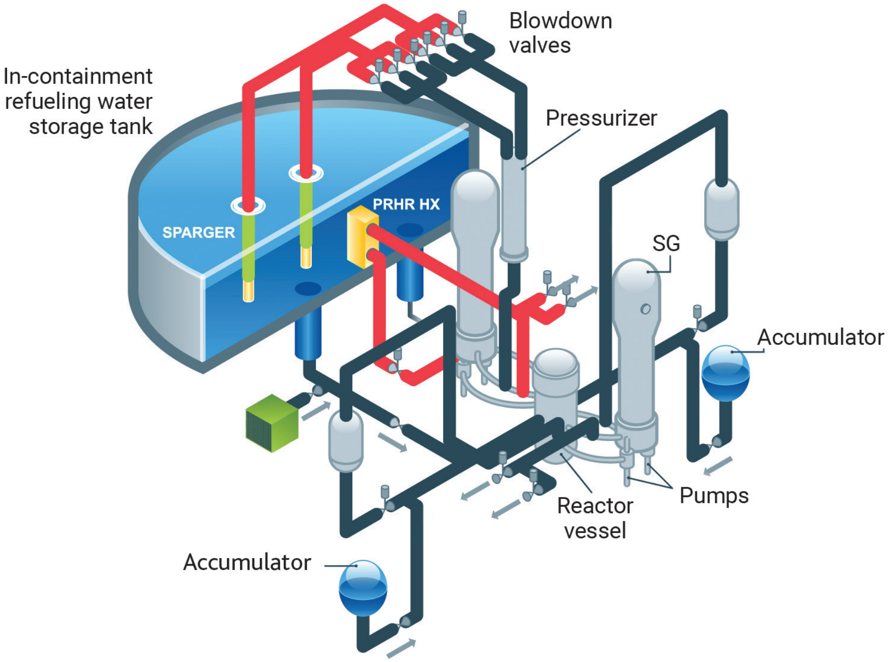


Figure 18.3. Diagram illustrating the gravity injection line in the AP1000. Westinghouse Electric Company LLC.

The containment cooling system is another interesting example of a passive system used in the design of the AP1000. This consists in a tank of 'clear' water, at ambient pressure and temperature, located in the upper part of the reactor building, above the reactor containment. Its function is to cool the containment and ensure that the temperature and pressure values remain within the design-basis ranges.

To this end, if there is any rise in the temperature inside the containment, the valves at the bottom of the tank open to allow the water in the tank to cover the outer surface of the containment, by the force of gravity. Vents are used to circulate air through the reactor building, counter to the water flow path, promoting heat transfer with the containment shell. The tank is designed to ensure passive cooling of the containment for 72 h.

Drains in the floor of the reactor building serve to collect water flow so that it can be recirculated after the first 72 h. The containment cooling system thus ensures the function for which it has been designed throughout the long term.

The passive systems introduced have clear advantages, but for each individual case, a review is required to demonstrate their effectiveness through representative tests, their resistance to external hazards, performance during outage states, their compatibility with periodic inspections, etc.

18.4.2. VVER: SPOT system

VVER units are pressurized water reactors of Soviet, now Russian, design, which have been developed since the 1960s, today by ROSATOM.

The system described in this section is the SPOT system (see Figure 18.4), which provides passive cooling of the steam generators in beyond-design-basis accident situations involving total loss of electrical power supplies. This system is only used in certain VVER-1000 and VVER-1200 units (with four reactor coolant system loops), which are among the most recently built models.

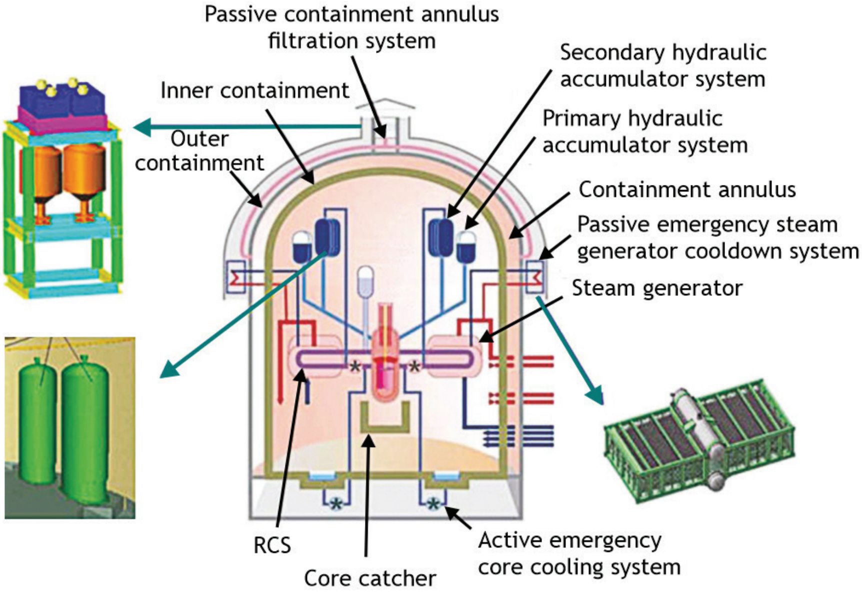

Passive containment annulus filtration system
Inner containment
Outer containment
Secondary hydraulic accumulator system
Primary hydraulic accumulator system
Containment annulus
Passive emergency steam generator cooldown system
Steam generator
RCS
Core catcher
Active emergency core cooling system

Figure 18.4. Diagram illustrating the SPOT system with air cooling. ROSATOM.

The SPOT system consists of four air-cooling heat exchangers, one on each loop, located outside the reactor containment at the top of the reactor building. Depending on the unit, these heat exchangers are in direct contact with the air (case of the VVER-1200 Novovoronej II-1, in service since May 2016 – see Figure 18.4) or are submerged in water tanks (case of the VVER-1200 Leningrad II-1, in service since October 2018). Whichever design is used, the system operates according the same principle: steam exiting the steam generators naturally rises to the heat exchangers, where it is cooled and condensed. The condensate then descends due to gravity to the lower section of the horizontal steam generators. The system is designed to ensure sufficient cooling using three out of the four heat exchangers during operation. In the case where the heat exchangers are submerged, the water tanks also serve to ensure passive cooling of the containment if loss of coolant occurs. For this purpose, heat exchanger-condenser units are installed in the upper part of the containment. The liquid water contained inside the condensers heats up and rises through natural convection to the tanks in which it will be mixed. Vents are installed to allow the water in the tanks to evaporate. The tanks are designed to cool the steam generators and the containment for a period of 24 h.

18.4.3. NM EPR: 'multi-group' technology, diversified heat sink

The new-model EPR (NM EPR) is a project developed by EDF and Framatome[615] that sets out to build a pressurized water reactor based on the EPR; it has not been finalized and project changes are already being planned by the developers under the name 'EPR 2'. While the general safety architecture for the new model is similar to that of the EPR, some of the changes planned are worth mentioning since they illustrate the progression of the safety approach.

In particular, design of the emergency power sources has changed, providing greater independence between defence-in-depth levels 3 and 4, which should therefore improve reliability of the safety function that removes decay heat from the containment in the event of a severe accident.

In addition to the main diesel generators, which supply power to safety systems if a loss of off-site electrical power occurs, the NM EPR will have emergency generators dedicated to managing station blackout situations based on multi-group technology. This technology will supply the required power level by interconnecting lower-power diesel generators to form a single functional assembly. The individual diesel generators will be identical, interchangeable and independent from one another. Each individual diesel generator will have a certain number of support systems of its own (such as the motor-cooling system, buffer fuel storage tank, etc.), designed to make the whole configuration more reliable, even though there will still be some shared support functions.

The emergency diesel generators will be designed to manage all accident situations for which they may be required, taking into account the simultaneous impact of accidents affecting the reactor and the spent fuel pool.

The systems used to respond to a core-melt situation will have an emergency diesel generator dedicated solely to this situation.

Regarding the heat sink, the NM EPR will have two heat sinks: the main heat sink, which will use a direct water intake from the natural environment (sea or river,

[615] In April 2016, EDF submitted to ASN the Safety Options Report for an 'NM EPR' reactor project, intended to follow on from the EPRs already built. For EDF, the aim of this project is to integrate feedback on the design, construction and operation of EPRs already built, together with feedback on existing reactors, thereby giving France's nuclear industry a reactor that affords high levels of safety as it looks ahead to renewing the fleet currently in operation in France. The Safety Options for the NM EPR project were reviewed in January 2018 by the Advisory Committee on Reactors. On 16 July, ASN published Opinion No. 2019-AV-0329 on the project and its evolution to the EPR 2.

depending on the site location) and will supply feedwater to the RCS, and a diversified air-cooled heat sink which will supply the diversified cooling system used under Design Extension Condition A (DEC-A) and the ultimate cooling water system under Design Extension Condition B (DEC-B). The aim of this design option is to eliminate the risk of common-mode loss of both heat sinks.

18.4.4. ATMEA 1: safety injection accumulators in the reactor coolant system

ATMEA 1 is a project to build a 1100 MWe pressurized water reactor jointly developed by Mitsubishi Heavy Industries and AREVA-NP. In 2011, the French Nuclear Safety Authority (ASN) issued a favourable opinion on the safety options set out for this reactor project in light of the preliminary design options for this reactor.

These options include an innovation that was introduced in the ATMEA 1 project to manage loss-of-coolant accidents. Unlike most pressurized water reactors, ATMEA 1 does not include an active low-head safety injection system (the primary aim of which is to reflood the core in the immediate term in the event of a large-break loss-of-coolant accident).

To fulfil this function, the ATMEA 1 project uses passive accumulators known as ‘two-stage’ accumulators, since they function in two successive injection stages. When activated, they release the water in the RCS at an extremely strong flow rate, to reflood the fuel within a matter of seconds. Once this first stage is complete, the accumulators continue to release water at a slower rate.

These accumulators are designed to provide sufficient injection to maintain core cooling until the medium-head safety injection pumps start up. The latter are used for the longer-term management of a loss-of-coolant accident. This operating mode is therefore used for design-basis conditions involving the loss of off-site power sources, to avoid having to use emergency power sources in a short space of time (within a minute or so), thereby reducing the risk of damage to the diesel generators under such conditions.

18.4.5. NuScale: common pool for modular reactors

Since 2010, there has been a rapid development of a new type of reactor: the Small Modular Reactor, existing in many different types of design.

A small modular reactor is a reactor with a low power rating, designed for series production and assembly in factories to facilitate on-site installation. The power rating of small reactors is generally lower than 300 MWe or the equivalent thermal output.

According to designers, small modular reactors are designed for locations where it would not be possible to build a high-output nuclear power plant, including at secluded sites. In addition, the low power rating makes them less costly than a large nuclear power plant, making them an attractive alternative for countries that wish to start a nuclear power-generation programme. Last, they have a small inventory of radioactive substances, which means they could be sited close to urban centres for which the combined generation of electricity and steam could also be viable.

The US firm NuScale Power is developing this type of design for a 50 MWe small modular integral pressurized water reactor. Reactor modules would be factory-built and then transported to the site for assembly in a single facility. The plan is to install up to twelve modules on a single site, possibly sharing certain auxiliary and safety systems. A NuScale power module is made up of a primary vessel that contains the reactor core, the pressurizer and two steam generators. The primary vessel is housed inside a containment vessel, which acts as the third physical confinement barrier. A vacuum is maintained between the reactor vessel and the inside of the containment vessel.

The design choice presented below features a common pool in which all the power modules would be submerged (see Figure 18.5).

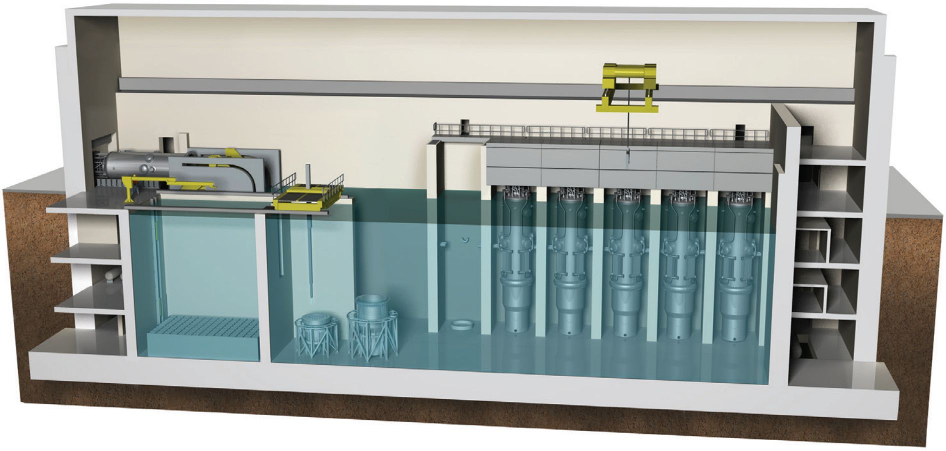


Figure 18.5. Illustration of the common pool for the NuScale project. Right: five power modules housed in their containment vessels. 2020 NuScale power, LLC – All rights reserved.

The decay heat removal system in each power module consists of two reactor coolant system trains, one for each steam generator. Each train is equipped with a condenser submerged in the common pool. Each condenser can remove 100% of the decay heat (see Figure 18.6).

If feedwater supply to the steam generators fails, a series of valves is used to isolate the affected module from the turbine and stop feedwater injection to the steam generators, while another series of valves opens to connect the steam generators, located inside the reactor vessel, to the two condensers submerged in the pool. The secondary coolant then circulates based on two-phase natural convection.

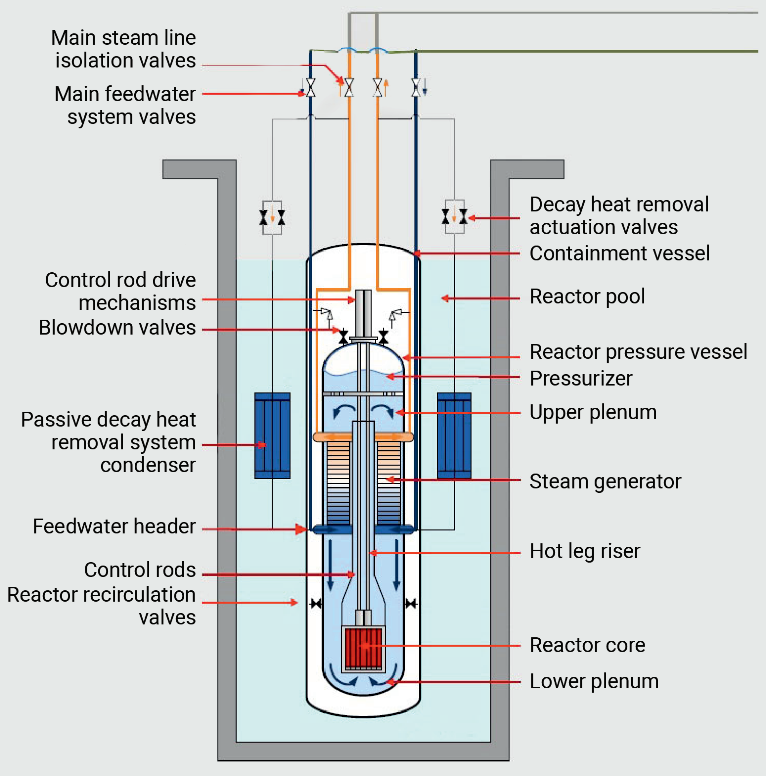

Main steam line isolation valves
Main feedwater system valves
Control rod drive mechanisms
Blowdown valves
Passive decay heat removal system condenser
Feedwater header
Control rods
Reactor recirculation valves
Decay heat removal actuation valves
Containment vessel
Reactor pool
Reactor pressure vessel
Pressurizer
Upper plenum
Steam generator
Hot leg riser
Reactor core
Lower plenum

Figure 18.6. Diagram showing decay heat removal for the NuScale project. 2020 NuScale Power, LLC – All rights reserved.

The common pool would be designed to ensure power module cooling under any design-basis incident or accident conditions for 72 h, without requiring any operator intervention. After 72 h, pool water boiling and evaporation, together with containment cooling by air, should be enough to ensure unlimited decay heat removal.

The designer also emphasizes that the pool may be thought of as a fourth confinement barrier, since it is designed to retain some of the fission products produced in the event of containment vessel failure.

Part 3

Safety in Operation

Chapter 19
Startup Tests for Pressurized Water Reactors

19.1. Introduction

As indicated in the appendix to Chapter 6, the Chooz A reactor, which had a power output of 300 MWe, was the first pressurized water reactor to be commissioned[616] in France. It first went critical on 18 October 1966 and its first connection to the grid was on 3 April 1967. During the period from 1970 to 2000, 58 pressurized water reactors for nuclear power generation were built and commissioned in France. After the first reactors at Fessenheim and Bugey[617], those that followed consisted of several series of standardized reactors (28 reactors in the 900 MWe series, 20 reactors in the 1300 MWe series, and four reactors in the 1450 MWe series). The last of these reactors to be commissioned was Unit 2 (a 1450 MWe reactor) at the Civaux nuclear power plant; its commissioning tests were completed during 2000 (Figure 19.1).

Successful completion of the startup tests is a major industrial challenge for the designers, builders and operators of these facilities. The startup test phase is relatively short, but much is learned in terms of design validation; analysis of any discrepancies[618] discovered during this phase makes a particularly large contribution to lessons learned.

[616] 'Commissioning' is declared by the power utility after the startup tests and connection to the grid.

[617] These were subsequently referred to as the CP0 reactors, in reference to the multi-annual programme contracts that followed.

[618] A finding or observation that does not meet requirements. This concept is explained in Chapter 29.

Conducting startup test programmes, evaluating their results and dealing with the problems encountered obviously contribute to achieving the facilities' desired overall safety level; these activities therefore need to be managed and controlled to ensure they are of sufficiently high quality. The value of startup tests for training the teams that will go on to operate the reactor is also important. These teams therefore need to be deeply involved in test preparation, in monitoring and analysing test execution and in learning lessons from the test outcomes.

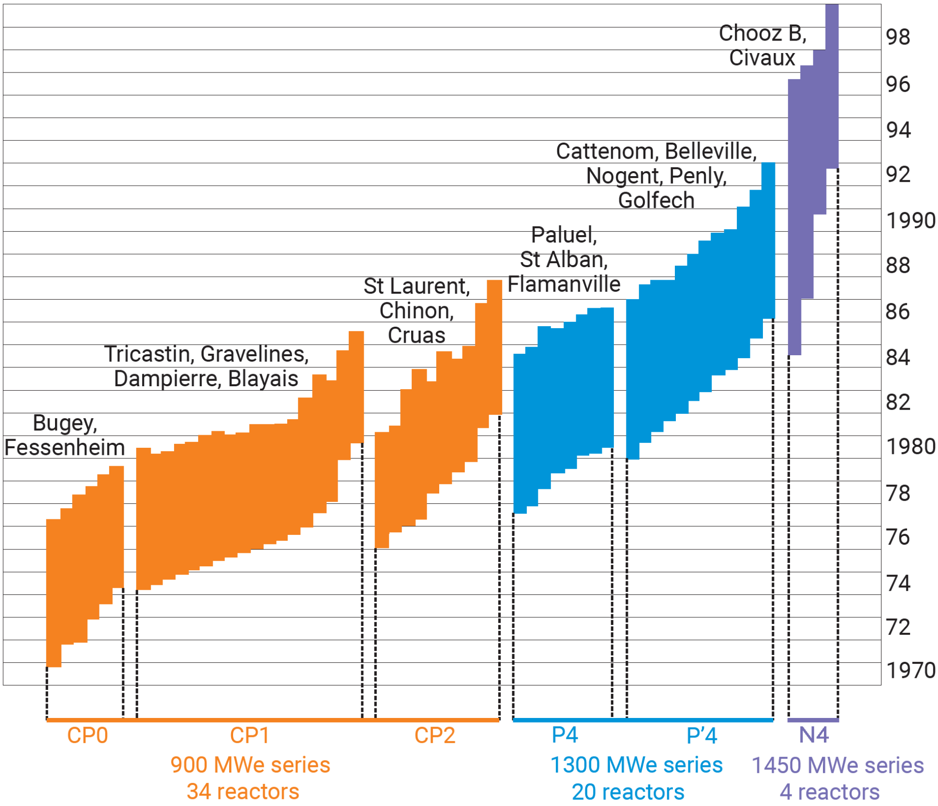


Figure 19.1. Chronology of the construction and commissioning of French nuclear power reactors. Georges Goué/IRSN.

From a safety point of view, startup tests provide an opportunity to verify facility compliance as built, and to check compliance of its operating procedures with specifications (or requirements in the sense of the 1984 Quality Order) defined and used for design and the safety demonstration. Before a facility of this kind is started up for the first time, the equipment and systems in place must be checked to ensure they have the expected characteristics and offer the required performance. But while tests of individual items of equipment, then of increasingly complex systems, are not a particular problem when verifying their characteristics in normal operation, it is much more difficult to check, for example, that engineered safety systems behave as expected in accident situations. It would obviously not be possible to make a guillotine break in a reactor coolant system pipe at 155 bars to check that the safety injection flow rates meet requirements. Nor would it be possible to deliberately flood the reactor building by starting up the containment spray system. Indirect methods of obtaining the corresponding information must therefore be found. This requires special analyses and transposing test conditions. For example, tests conducted on low-head safety injection pumps and accumulators take place when the reactor vessel is open, which corresponds to conditions in which the reactor coolant system is completely depressurized. Under these conditions, the maximum flow rate of the pumps, with the systems' actual head loss, can be assessed and recalculated for accident conditions. The containment spray system is tested using temporary pipes that divert the water into the reactor building sumps, in order to check that the system pumps operate correctly. The spray nozzles, which are blocked during testing, are checked separately by measuring flow rates using compressed air.

The tests required by pressure equipment regulations – such as increasing the pressure above the 'design pressure' (see Section 8.6) or setting it at the level for finding and assessing leaks – are included in the test programmes.

The operator draws up the test programmes, including the sequence of tests to be performed on each system and the tests conducted on the entire facility. This means writing approximately 100 system test-principle programmes, and for each of these, around 15 test procedures, i.e. around 1500 documents per reactor. Each of the tests to be performed is scheduled for the appropriate phase of commissioning.

Since the first nuclear reactors were commissioned, French safety organizations have closely monitored the preparation of test programmes, test execution and analysis of test results, particularly during the startup test phase (this concept is explained in more detail in Section 19.2.1). For each new pressurized water reactor series, the test programme content was analysed by IPSN. The content improved in light of experience gained with previous series. Particular attention was also given to the 'on-line' analysis of the results of tests performed on site.

In this regard, in 1966, Jean Bourgeois, chairperson at the time of the French Atomic Energy Commission's Pile Safety Commission, secured the presence on the Chooz site of an engineer from the Pile Study Department to monitor what was referred to as the 'operational tests' (see Section 19.2.2.2 below for a definition of these tests). Similarly, all the tests (startup, power escalation, operation at power) conducted on the site of the PHENIX sodium fast-neutron reactor in Marcoule in 1973 and 1974 were monitored by an engineer from the French Atomic Energy Commission's Nuclear Safety Department. Since all the parties recognized the effectiveness of this process, an engineer from the French Atomic Energy Commission's Nuclear Safety Department was also seconded to the site for the startup and power escalation tests of the first reactor at the Fessenheim nuclear power plant. IPSN was then involved in the startup of the other 57 reactors at France's nuclear power plants.

IPSN carried out its analyses of the test results by relying on its presence at the corresponding sites and on its in-house experts, working consistently with Électricité de France's (EDF) engineering and design departments. The IPSN engineer assigned to a site still took an analytical approach, but being on site made it easier to conduct technical reviews of the test programmes and procedures, in particular by checking that test sequencing in the different startup test phases was correct, by examining test results in real time to check compliance with safety requirements and criteria, and by making sure tests were only started once satisfactory results had been obtained in earlier tests. The engineer also played a part in reviewing requests for temporary changes necessary to perform the tests. This method of organization proved flexible and effective. For this reason, similar arrangements were used for tests conducted on the Flamanville 3 EPR.

The rest of this chapter explains various aspects of the startup tests carried out on pressurized water reactors, presents a few findings from the experience of conducting startup tests on the 58 reactors in the 900 MWe, 1300 MWe and 1450 MWe series, and explains the resulting adjustments and improvements made over time. The startup test programmes for the Flamanville 3 EPR are also discussed, and particularly the benefits to be gained from conducting long-term endurance tests on equipment important to safety.

19.2. Commissioning

19.2.1. Defining startup tests

When a nuclear power reactor such as a pressurized water reactor is being commissioned, EDF carries out inspections and tests (or has them carried out on its behalf), in particular of items important to safety[619], whether they are structures, systems or components (SSCs), referred to hereafter as 'equipment'. These tests include:

- inspections and tests conducted outside the perimeter of the basic nuclear installation on equipment important to safety, during its construction (including inspections of large components such as pressurizers, steam generators, etc.),
- inspections and tests carried out within the facilities during the assembly, construction or installation of this equipment,
- inspections and tests carried out within the facilities once this equipment has been installed, referred to as '**startup tests'**.

[619] The concept of equipment important to safety (EIS) has been used for all 58 reactors set into operation in the nuclear power plant fleet. Since the Order of 7 February 2012 introducing general rules for basic nuclear installations (the INB Order), the concept to be used has been 'items important to protection' (see Section 2.2 of this book). The operator also ensures that inspections and tests are conducted on equipment, components and systems used to generate electricity (the 'conventional' part of the facility).

The purpose of all these tests is to check that the facilities as built comply with the requirements adopted during the design phase and in the corresponding safety demonstration, as defined in:

- the applicable regulatory texts,
- the operating authorization application, which includes the (updated) safety analysis report and the general operating rules, submitted before the startup tests are performed.

Generally, defining the startup tests requires, for each item of equipment:

- identifying all its conceivable operating configurations,
- identifying, for each operating configuration, the corresponding functional requirements,
- incorporating the identified requirements in the test conditions.

These configurations must be included in the elementary tests of the relevant equipment, or in integrated system tests conducted on systems that use this equipment.

The strategy and procedures for carrying out startup tests naturally benefit from lessons learned from tests performed previously and take into account the facility's specific characteristics. Therefore, for example, when the startup tests of the Flamanville 3 EPR were carried out:

- greater use was made of the instrumentation that would be used in the operational phase (which was more precise than that of previous reactors and therefore reduced the need for special test instrumentation),
- startup tests were carried out on passive systems.

19.2.2. Phasing of startup tests

Without going into detail about the phasing of startup tests on French pressurized water reactors, it is useful to recall that they can be divided into three phases consisting of **preliminary tests** performed on equipment, **pre-operational tests** performed before the core is loaded, and **operational tests**. The sequencing of the phases and tests is summarized in Plates 19.1 and 19.2 at the end of this chapter.

19.2.2.1. Preliminary and pre-operational tests

The preliminary and pre-operational tests start once assembly operations have been completed. They aim to check that the equipment and functional systems are operating correctly and to take any necessary corrective actions if malfunctions are detected. The test programme consists of all the tests, inspections, tuning, adjustments and functional tests necessary for core loading to take place, followed by the first state of criticality and the low-power tests, performed under satisfactory safety conditions. Initially, specific operating conditions can be used to carry out tests (such as 'no-load' testing of a motorized valve, i.e. without fluid flow); as the tests progress, new functional parts of the facility may be added, approaching normal facility operating conditions. Where possible, abnormal operating conditions are also simulated, provided that they do not compromise personnel safety, equipment integrity or the cleanness of system lines. The value of these preliminary and pre-operational tests is that they are performed under operating conditions (in terms of temperature and pressure) often not very different from normal reactor operating conditions, achieved by means of the pumping power of the reactor coolant pumps that drive the reactor coolant. Because these tests are carried out without the core loaded, they pose no problem in terms of nuclear safety.

The preliminary tests of equipment and portions of systems, once assembly has been completed, consist of checking fluid supplies (water, air, electricity, etc.), carrying out 'wire-by-wire' testing of electrical circuits (see Figure 19.2), performing tests on instrumentation and control systems, initial operation tests on actuators, pump rotation tests, making sure system lines are clean, etc.

Figure 19.2. Operators inspecting electrical cables in the Flamanville 3 EPR. Alexis Morin/IRSN Media Library.

The pre-operational integrated system tests conducted on the main systems (including the safety injection system and containment spray system) check in particular that these systems have been correctly dimensioned by ensuring compliance with safety criteria incorporated in the test conditions. Integrated system tests of the main primary system are then carried out by means of 'cold' functional tests including the strength and leak test, which is a regulatory test, and 'hot' functional tests during which the main primary system (without the fuel and rod cluster control assemblies) and its associated systems are tested under nominal operating conditions in terms of temperature and pressure, to check that the safety functions are available.

These tests include specific tests (loss of electrical supply, failure of instrumentation and control systems, compressed air, etc.) to validate the design assumptions used and the operating instructions associated with these incident situations.

19.2.2.2. Operational tests

Operational tests are performed after the first core loading; they consist of:

- cold then hot pre-criticality tests, which complete the preliminary and pre-operational tests as regards, in particular, correct operation of the rod cluster control assembly control mechanisms and the settings affected by the presence of fuel;
- criticality followed by power escalation tests to check that the facility performs correctly both functionally and in terms of safety. This stage consists of reaching core criticality, connecting to the grid, and conducting physical tests of core compliance as well as adjustment of the reactor control and protection parameters during power escalation from initial criticality to operation at nominal power.

19.2.2.3. General principles for test sequencing and execution

The order in which the different tests are carried out is specified by the integrated system test procedures (pre-operational tests) and startup procedures (operational tests), which call up the Test Procedures (TPs). The order in which the tests are conducted depends on the conditions and imperatives of their execution. This facilitates test scheduling, which is adjusted on a daily basis. The following rules must be followed:

- the reactor must not be brought to a state in which its safety depends on the performance of equipment that has not yet been verified;
- all the pre-operational tests must have been completed before the first fuelling of the reactor. However, testing of equipment or systems that can only be installed after fuelling (such as rod cluster control assembly tests) are the exception to this rule. For this reason a full set of cold and hot pre-critical tests is conducted after core loading and after the closure head has been sealed, before the actual startup of the reactor;
- tests are carried out in stages such that the satisfactory performance of one stage demonstrates that the next one will be safe; for this reason, each stage must be pushed as far as possible, where appropriate, by simulating certain operating parameters (such as core head-loss in operation during the pre-operational integrated system tests, using filter blocks fitted inside the vessel);
- the operator must validate the (normal and incident) operating procedures and the periodic test procedures as the tests progress – the emergency operating procedures are validated using a simulator or simulation software.

Where, due to unavailability, a pre-operational test cannot be conducted normally before the core is loaded, or where the results of a pre-operational test are not considered satisfactory, the test may, exceptionally, be conducted or repeated after loading, provided that this would not compromise compliance with safety requirements.

Tests are conducted in such a way that they will not cause or risk damage to equipment integrity: for example, pump tests are performed without going as far as fluid cavitation.

If a test of a system that includes, for example, a chain of actuators, can only be performed in sections, any partial tests of the system must overlap each other.

19.2.3. Documentation for startup tests

19.2.3.1. Integrated system test procedures and startup test procedures

As stated earlier, integrated system test procedures and startup test procedures are used to plan the build-up to nominal conditions in terms of pressure, temperature and nuclear power; chronologically, they call up all the test procedures to be performed at the appropriate time, and also the corresponding periodic tests to be validated. They are used to coordinate the progress of tests on the nuclear part and the conventional part of the facility. They are the tool used for scheduling startup tests on site.

19.2.3.2. Test programmes, test procedures, standard test guidelines

The comprehensive startup test programme is organized according to elementary plant system[620], equipment type (pump, valve, etc.) and cross-cutting subject matter (for instance, verification of facility behaviour in the event of an electrical power supply failure). The tests to be conducted are then defined more precisely in the system test-principle programmes and standard test guidelines:

- for a given elementary plant system, the test programmes present the objectives of the planned tests, their sequencing, the principles for conducting these tests and the test criteria used to check system compliance, given in the test procedures;
- standard test guidelines describe the procedure to be followed for tests of the same type to be performed on different categories of equipment (electrical motors, pumps, fans, valves, etc.).

19.2.3.3. Completeness analysis, adequacy analysis

For the 58 reactors in operation in the nuclear power plant fleet, EDF defined the tests to be performed, based on elementary system files that describe the design principles of the equipment and specify the (safety) functions it must be able to fulfil. To

[620] An elementary plant system is a group of equipment items that performs a common function, such as safety injection, spraying water in the containment, ventilating a building, etc.

ensure the planned tests were exhaustive, EDF identified all the 'assertions'[621] made in the elementary system files and linked each of them to one or more tests to check them, assigning an acceptance criterion to each. EDF also checked that all equipment identified functionally in the elementary system files would be tested as regards its ability to ensure the safety functions that it was designed to fulfil. This analysis is traced in completeness analysis reports.

In addition to this system-based approach, EDF set up a 'thematic' analysis by creating test programmes of 'pseudo systems', in order to test nuclear reactor and turbine control functions, loss of electrical supply, measurement of pipe vibrations, etc.

Developments involving test completeness will be discussed further in Section 19.4.

For the Flamanville 3 EPR, EDF used a new method to check the completeness of the planned startup tests. This is known as the Adequacy Analysis method, traced in adequacy analysis reports. The aim is to substantiate the sufficiency of factory inspections and the planned on-site tests and inspections conducted to check compliance with the safety requirements applicable to systems and their various components. Adequacy analysis reports specify the safety criteria to be met during tests and inspections. In most cases, adequacy analysis reports were drawn up for each elementary plant system, based on an analysis of safety functional requirements, which identifies all the requirements applicable to the system mentioned in the safety analysis report. Configurations affecting several elementary plant systems (such as loss of instrumentation and control switchboards) are treated as 'pseudo systems' (for example, the pseudo instrumentation and control system is referred to as 'pseudo system COC'), which are also examined in an adequacy analysis.

19.2.3.4. Acceptance criteria

The results of a startup test are assessed by comparing the results of measurements and observations made with predefined acceptance criteria. These criteria, which may be qualitative or quantitative, fall into four categories:

- S criteria: criteria for which non-compliance invalidates the studies presented in the safety analysis report,
- I criteria: criteria for which non-compliance could lead to the malfunction of an item important to safety,
- R criteria: criteria to assess test representativeness,
- C criteria: contractual criteria.

As explained above, it is not always possible when conducting tests on site to reproduce the worst-case operating conditions used in the design studies to determine the necessary performance of equipment (for example, a fluid flow rate value to be

[621] For example: ...pump X performs cooling at a flow rate of x L/h... or ...the command to close valve Y comes x seconds after threshold S has been exceeded...

guaranteed in accident conditions); it is therefore necessary to transpose the values given in the safety demonstration to the test conditions in order to define appropriate acceptance criteria.

19.3. Objectives and general rules to take into account for startup tests

When defining startup tests, it is important to:

- identify clearly and exhaustively the safety functions and associated safety requirements of each item important to safety;
- determine all the conceivable operating configurations in normal, incident and accident conditions for each item important to safety;
- establish, for each of these configurations, the corresponding functional requirements for the equipment (minimum or maximum flow of a fluid, admissible ranges of variation, valve opening with a maximum pressure difference, valve closing at full flow, etc.);
- define tests to be performed and their sequencing, and check their completeness; each functional requirement must be validated; this can take the form of a study, a 'qualification'[622] test, a startup test or a combination of all three, bearing in mind that, where possible, validation should preferably be achieved by means of on-site tests, which are more conclusive;
- ensure the tests carried out for different items important to safety are consistent; ideally, the validation methods involving testing used by the different designers of this equipment should be compared;
- adapt the criteria to the test performance conditions, seeking to make the tests as representative as possible;
- take into account the uncertainties associated with measurements taken during the tests when defining criteria and interpreting results;
- analyse very carefully the relationships between equipment in different systems, to ensure the tests validate overall operation, or add tests for this purpose;
- take into account lessons learned from previous startups and reactor operating experience, including at international level (publications, IRS[623] database, etc.);
- during testing, carry out periodic tests and routine maintenance operations planned to take place during reactor operation;
- validate operations documents;

[622] This concept was explained in Section 7.4.3. See also Section 19.4.1.

[623] International Reporting System for Operating Experience – see Section 3.1.3.

- examine any waivers from the operational limits and conditions that are required to perform certain tests, as well as the use of any temporary measures and devices[624].

Some of these aspects are explained in more detail in the next section, illustrated by operating experience feedback from the startup of the different reactor series.

19.4. Key lessons learned from startup tests on nuclear power reactors in France

From the drawing up of the test programmes for the first 900 MWe reactors to the commissioning of the last reactors in the N4 series, startup tests have been the subject of much reflection and discussion.

Experience with the startup of the first 900 MWe units showed the importance that should be given to defining startup test programmes. In the early 1980s, the Central Service for the Safety of Nuclear Installations set up a working group on the subject with EDF and IPSN. This working group's conclusions highlighted:

- the importance of startup tests for obtaining knowledge on the behaviour and quality of facilities,
- the value of startup tests for training personnel,
- the need to define a method for drawing up test programmes and to clearly define the conditions for starting equipment tests in view of the assembly phases of this equipment,
- the benefits of making better use of tests conducted in the past on reactors in the startup phase (comparison of results, difficulties encountered, etc.).

In particular, the working group considered that it was important to ensure the startup tests were exhaustive, as already explained from a documentary point of view in Section 19.2.3.3. A method was implemented starting from the initial tests conducted on 1300 MWe units.

Despite the care taken in defining test programmes, startup tests on the four reactors at the Paluel nuclear power plant (type P4 1300 MWe reactors), by chance, revealed a number of problems, confirming the importance of staying vigilant during equipment qualification and allowing sufficient time for testing.

The discovery in 1990 of major anomalies during startup tests on other 1300 MWe units (poorly installed filters in the containment sumps, installation of plugs instead of diaphragms in the U5 containment filtered venting system used in the event of core melt, etc.) prompted EDF to take action to improve:

[624] For example, temporary connections, jumpers, etc.

- the exhaustiveness of the startup test final verifications, by means of a completeness analysis, starting from the startup tests at Golfech Unit 2, and an examination of the test ‘coverage’ on equipment that would be used if procedures related to beyond-design-basis situations were applied (H and U procedures),
- the qualification procedures for systems and functions that cannot be tested in their expected conditions of use.

At the time, there was no established policy on the completeness analysis method. Following initial discussions on the test programmes for the N4 series and taking into account issues regarding the validation of safety measures that could not be checked through testing, raised mainly because of anomalies observed on engineered safety systems, the completeness analysis method was improved. EDF made an effort in particular to cover generic subjects (testing valves important to safety, measuring vibration levels in system lines, endurance tests on engineered safety equipment, etc.). As regards correct identification of all the requirements associated with equipment and systems, the functional and physical approach used for the N4 series units was more systematic and precise than the approach used for previous series.

The sections that follow present a history of the issues requiring attention and the lessons learned from startup tests, illustrated by analyses of the test programmes and feedback from test outcomes.

19.4.1. Qualification tests and on-site tests

As indicated in Section 7.4.3, ‘qualification’ for equipment important to the safety of a nuclear reactor aims to verify its aptitude to fulfil the roles assigned to it in normal, incident and accident operating conditions, and in the event of hazards (earthquakes, etc.). The qualification programme for this equipment lists the tests and analyses to be performed on a model of the equipment that will be installed on site. Reference characteristics can also be obtained during the qualification programme, and each item of equipment manufactured is then factory tested against them. The inspections and tests carried out when the equipment is installed on site in its environment (compliance with installation requirements, performance tests, etc.) and integrated system tests are conducted in addition to qualification. It is therefore necessary to examine carefully how the qualification tests and the startup tests complement each other in order to obtain appropriate evidence that the equipment operates correctly and delivers the required performance in its conditions of use, including the relevant accident situations. In practice, a policy should be defined regarding on-site verification of the characteristics of components included in systems important to safety, especially taking into account the qualification tests and factory acceptance tests carried out on these components, to avoid shortcomings or unnecessary redundancy.

Startup tests must be carried out under conditions that are as close as possible to operation, and equipment that is factory tested must be tested functionally once installed on site. On 21 August 1992, during a periodic test of hot shutdown operation following a shutdown for refuelling of Unit 1 at the Cruas-Meysse nuclear power plant, damage was caused to the turbine-driven pump of the emergency feedwater system (EFWS) because of a lubrication problem. A ‘lubricating oil low pressure’ alarm should have alerted the operator, but the pressure switch tapping had not been installed in the correct location and therefore the alarm was not operational. This anomaly also affected the other three units at the Cruas-Meysse nuclear power plant and dated from the time of construction. The pressure switch had been factory tested by the manufacturer but had not undergone real testing after it was installed on site. Because of this, the installation error had never been detected because testing of the alarm in a real situation had not been required. The anomaly was only detected by chance during periodic testing because it pointed to a lack of lubrication oil.

For all the plant series, problems have been identified on site during initial testing of certain equipment used under normal operating conditions: diesel generators, intake and control devices for turbine-driven pumps in the emergency feedwater system, motor-driven pumps in the same system, turbine alternator for the pump that injects water into the reactor coolant pump seals, etc. This has led to many corrective actions and engineering changes, accompanied by requalification, in the course of commissioning of the corresponding units. Although these problems have not required replacement of the equipment concerned, resolving them by making changes has proven difficult before commissioning the incriminated unit. Some corrective actions were only validated during startup tests on later units. In certain cases, malfunctions were not detected on the first unit of a series: for example, with the N4 series, problems with the diesel generators appeared during tests on the reactors at the Civaux nuclear power plant, equipped with a new type of diesel generator. These problems raised questions regarding the validity and effectiveness of factory tests. In principle, these problems could have been avoided if pertinent qualification tests in normal, incident and accident operation had been conducted very early on a few items of equipment chosen from those for which there was no standard industrial application or where the standard industrial application was too different from the planned use. This means that special attention should be given to the content of factory qualification tests by taking into consideration operating experience pertaining to the equipment in question.

Design anomalies affecting engineered safety equipment that would be used in accident situations have been identified during on-site testing, highlighting the inadequacy of qualification tests carried out at the factory or on a test loop. For example, the design anomaly affecting motorized valves in the safety injection system of the (type P’4) 1300 MWe reactors was discovered by chance following investigations on site during the startup tests at the Nogent-sur-Seine nuclear power plant. This anomaly, due to incorrect sizing in reactor design, had not been identified during qualification tests on a loop because the situations tested did not cover bounding conditions. It caused EDF to make significant design changes (replacement of a large number of motors on the various reactors affected). This anomaly is explained in more detail in Section 19.5.

It is also important to note that when startup tests (and also periodic tests) are carried out in a normal situation, they may not detect anomalies that would only have consequences in an accident situation. On 12 November 1991, when Unit 2 at the Cruas-Meysse nuclear power plant was shut down for refuelling, it was discovered during a maintenance operation that there were filters on the intakes of the EFWS turbine-driven pump and the motor-driven pumps in the same system. Checks revealed that similar filters were present on the intakes of the motor-driven pumps and turbine-driven pumps of the EFWS on units 3 and 4. These filters had been installed during initial startup when the pipes were flushed, and had not subsequently been removed. Their presence was not detectable by the startup or periodic tests. If raw water had been used in an accident situation, the filters could have become clogged, causing damage to one or more of the EFWS pumps.

19.4.2. Long-term on-site testing

During the startup tests on the 900 MWe reactors, lubrication and coupling problems between the motors and the high-pressure safety injection pumps were identified because of the continuous use of this equipment for reactor coolant system makeup. Similarly, with the 1300 MWe reactors, certain problems could only be detected after long-term operation on site. For example:

- excessive vibration and rotor lift of the engineered safety motor-driven pumps (safety injection system [SIS] and containment spray system [CSS]),
- malfunctions related to lubrication conditions on the splined transmission couplings during endurance tests performed on these vertical shaft pumps,
- problems due to insufficient lubrication of the essential service water system pumps,
- problems with cooling of the emergency feedwater pumps.

This shows that the planned duration of the tests may not be long enough to confirm that certain equipment items are suitable for real operating conditions. The validity of the design of certain equipment items has been demonstrated by long-term testing on site. This was the case, for example, with the demonstration of the acceptability of high vibration levels in the spent fuel pool cooling system (FPCS) pumps. The pumps were tested for 8000 h of operation.

After high vibration levels and rotor lift were observed in 1985 in a containment spray system (CSS) pump during a 2000-hour test as part of startup testing at Saint-Alban Unit 2 (a P4 1300 MWe reactor), the safety organizations took the view that, whereas factory tests verified the performance defined at the design stage and whereas tests in a specialized loop (at Nantes-Indret's ECAN[625], at the EDF centre in Gennevilliers, etc.) verified the equipment's ability to withstand accident conditions, verification of its ability to withstand real operating conditions required a test of about 2000 h at least (continuous, if possible). Extended periods of operation are indeed

[625] *Établissement des constructions et armes navales* (which became DCN, DCNS then Naval Group in 2017).

necessary to test equipment in interaction with its environment (ambient conditions, effects of the actual suction and discharge systems, auxiliary cooling systems, etc.) and possibly reveal anomalies that were not identified during shorter tests. This is particularly important for engineered safety motor-driven pumps that never operate for extended periods during normal reactor operation. The safety organizations considered that on-site endurance tests should be carried out on this equipment as part of 'first-off' plant unit tests, and EDF was asked to examine this possibility for the N4 series.

In view of these lessons, EDF carried out extended on-site operating tests of equipment for the N4 series reactors:

– for Unit 1 at the Chooz B nuclear power plant, a containment spray system pump underwent a satisfactory endurance test (of 1500 h) in a minimum flow configuration to the FPCS tank, having been subjected to the equivalent of 16 years of periodic tests by carrying out the corresponding number of starts and stops (the pumps then underwent expert assessment at the factory);

– for Unit 2 at the same nuclear power plant, a safety injection pump underwent a satisfactory endurance test (of 1500 h) in a minimum flow configuration to the FPCS tank;

– for the same reactor, a diesel generator underwent a satisfactory endurance test (of 1000 h) consisting of 100 cycles of 10 continuous hours.

In the case of the Flamanville 3 EPR, having noticed that the startup test programme had clearly regressed in terms of long-term tests compared with the programme for the N4 reactors, and in view of the operating experience feedback from IRSN regarding vibration problems on engineered safety pumps, ASN asked EDF in 2018 to propose first-off plant unit on-site endurance tests for the engineered safety pumps and diesel generators that were not continuously in service during normal operation, considering worst-case conditions of mechanical, thermal and vibratory stress.

The topic of vibrations and rotor lift in safeguard pumps is discussed in detail in Section 19.5.

19.4.3. Test configurations and completeness, transpositions

As stated earlier, the method used by EDF to prepare test programmes aims to identify all design 'assertions' and as far as possible to include corresponding tests to confirm them. Detailed justification must be provided when tests cannot be conducted to verify certain assertions, especially when the assertion is based on a new concept or an operating configuration for an item of equipment important to safety that has not been tested previously. In this case, the benefits and feasibility of a functional test should be examined.

Generally, for the 1300 MWe reactors, EDF defined test configurations more comprehensively than for the 900 MWe reactors, especially as regards checking how the loss of fluid supplies (electricity, compressed air) impacts system lines. When it defined the test programmes for the 1300 MWe reactors, EDF conducted an analysis of usage configurations for certain systems that included, in addition to normal operation, operation corresponding to the limit conditions defined in the operational limits and conditions, as well as accident conditions and periodic test conditions. This exercise was rapidly extended to systems important to safety, leading to an extension of the test programmes beyond the scope covered in the 900 MWe reactor test programmes.

Following the discovery in 1990 of anomalies in engineered safety systems during startup of the P4 1300 MWe reactors (defective fabrication of sump filters, etc.), the method used to analyse completeness of the test programmes was improved for the N4 series with regard to safety provisions that could not be verified by testing the relevant systems in the real-life operating conditions for which they were designed. In particular, a complete review of the equipment and systems that would be used in beyond-design-basis situations (H and U operating procedures) but that had not been tested in real conditions of use, was carried out. This review consisted of three phases:

– analysis of the situations in the H and U procedures in which the equipment and systems not tested in real conditions would be used,

– grouping these situations according to elementary plant system,

– definition of additional tests or inspections to be carried out.

The main conclusions of these studies called for additional tests to include water makeup to the reactor coolant system, the reactor cooling modes, and restoring power supply to equipment and systems. These tests were included in the documentation either by modifying existing test procedures or by creating new ones.

Some systems are designed for operating conditions that are difficult to create during on-site tests; it is therefore necessary to extrapolate test results to fit these operating conditions. This is the case, for example, with the engineered safety systems (safety injection system, emergency feedwater system, containment spray system). The design-basis configuration for the medium-head safety injection (MHSI) pumps is the configuration in which a branch of the reactor coolant system breaks and is depressurized. In this case the head-loss in the pipes is measured on site, while the pump characteristics are those measured during factory tests. Based on these results, calculations are conducted to demonstrate that the system has been adequately designed.

One particular issue is how to consider equipment operation during transients. In the 1300 MWe reactors, hammering in systems such as the containment spray system (CSS), the component cooling water system (CCWS), and the essential service water system (ESWS) caused damage to those systems when transients occurred during startup tests. One of the causes of these events is the positioning of flow-limiting diaphragms at the top of the spray columns in the CSS. In a steady state this positioning does not pose a problem, but the same is not true when the system is started up and the water column rapidly arrives at the diaphragms, causing their deformation. These events showed that it was necessary to know and confirm at the design stage the admissible pressure values in the system lines and the methods for selecting the transients to be calculated (changing power supply sources, changing train, equipment failure, etc.). It is interesting to note that most problems of this type have been discovered by chance, even though, after the event, designers confirmed that the conditions encountered during the hammering events were by far the most pessimistic conditions. Design analysis should have led to taking into account these transient conditions by identifying the worst-case configurations, and should have called for planning the relevant tests during reactor commissioning. As a result of these events, special tests were carried out on Unit 1 at the Chooz B nuclear power plant.

19.4.4. Safety measures that cannot be verified by testing

As stated in the previous section, anomalies in engineered safety systems identified on startup of P4 1300 MWe reactors raised questions for EDF about the qualification of systems and functions that cannot be qualified by testing under real operating conditions. EDF carried out a complete review of the corresponding items and systems. The conclusions were presented above. During this process, EDF reviewed 'equipment not identified functionally because it does not play a role in the process' (self-locking devices, devices to support pipes in the reactor coolant system, etc.). For this equipment, it adopted a cross-functional technological approach and introduced inspections for certain measures. Hence, procedures were developed to:

- check that train A and train B electrical systems are independent from each other,
- check fire protection measures, especially the integrity of fire compartments,
- test the leaktightness of fluid-retaining devices,
- verify the displacement of pipes expected when the reactor changes state.

These procedures were maintained for the N4 series and further checks were added, for example:

- check the availability of valves and vacuum breakers,
- check the state of waterstops between buildings,
- check for any measures and devices put to use temporarily,
- check for lead seals prohibiting access to the settings on protective devices for actuator power supply units,
- check for unwanted retention points in the reactor building that would prevent water from returning to the containment sumps.

19.4.5. Criteria

For startup tests on 1300 MWe reactors, the definition of the test success criteria was significantly improved. Various names had been given to the test success criteria (safety criteria, design criteria, technological criteria, operational criteria and even expected values), but only the expression 'safety criteria' seemed to be clearly defined, although its definition was very restrictive. Only the values of parameters appearing in the assumptions of the accident studies presented in the safety analysis report were considered to be safety criteria. The definition of the test success criteria was improved (see Section 19.2.3.4), as was the procedure to be followed if these criteria were not met, in terms of analysis and declaration to the safety regulator.

Leaving aside compliance with criteria, it is often possible to learn as much from the difficulties encountered during testing as from the results themselves. Two examples from startup testing on 900 MWe reactors can be given to illustrate this. The first concerns the steam-line isolation valves, which should close in less than five seconds. The results of the on-site tests conducted, after extremely careful preparation of the valves by the manufacturer, showed that all the valves closed in less than five seconds and this equipment was therefore declared suitable to perform its function. It was not until an inspection was conducted that the operator reported that, without this careful preparation, closing time was much longer. The second example is similar and concerns the compressed air system (SAR) in the reactor building, which could only be made properly leaktight after around ten attempts, until EDF modified the system. It had nevertheless been possible to write a test report stating that the criterion was met. The safety organizations issued a reminder of the need to write test reports presenting not only results but also difficulties encountered, and in particular any observations that would cast doubt on the ability of equipment and systems to perform their functions later on.

In addition, some events that seem innocuous in normal operation (for example, a discordance in the device position [valve open or closed, etc.] reported locally and in the control room, a slightly longer valve actuation time than expected, etc.) are sometimes symptoms of malfunctions that could have serious consequences in an accident situation. It was difficulties with opening and closing valves in the safety injection system of Unit 1 at the Nogent-sur-Seine nuclear power plant in November 1986, during functional tests of the unit in a vessel-open configuration, that revealed design and qualification anomalies in certain valves in the safety injection system of 1300 MWe reactors. More than 30 valves on each unit had an undersized motor-drive system because the system design had been changed without updating the parameters taken into account for the choice of servomotors, and because the systems transmitting the remote-control signals were incorrectly sized due to a lack of knowledge of the effects of the motor's inertia on those systems.

19.4.6. Cleanness, keeping system lines clean, foreign matter

Since the first 900 MWe reactors were started up, EDF has had issues with system cleanness. For example, in 1980, during the first cold test of Unit 1 at the Le Blayais nuclear power plant, various types of foreign matter, such as pieces of a plug used by welders to form an argon welding chamber, were found in the vessel. After a detailed inspection of the reactor coolant system, the rest of the plug was discovered in a check valve in the safety injection system. The Central Service for the Safety of Nuclear Installations asked EDF to:

- define precautions to be taken during equipment installation, particularly for systems such as the main feedwater system where it is only possible to drive out foreign matter into the steam generators themselves,
- specify the minimum readiness to be achieved before system flushing and testing begins,
- examine the possibility of systematic inspections of places where foreign matter could be trapped (valves, tanks) after initial flushing,
- define strict procedures for working on systems assumed to be clean (marking out the work area, providing protection against falling objects, taking inventory of tools and parts used), clearly defining the phase from which these procedures must be applied.

In addition, in August 1986, during an inspection in the Unit 2 building at the Flamanville nuclear power plant, which had just been refuelled, the operator noticed that the sleeve (600 mm in diameter) of a penetration through a concrete wall, used in accident conditions to take condensed water from containment spraying to the sumps and thus to supply the SIS and CSS systems, had been blocked with a plug. A similar finding was then made for Unit 1 at this nuclear power plant. Obviously, it was immediately repaired and checks were carried out by EDF on other reactors potentially affected. The plugs found seem to have been the consequence of a campaign to plug openings carried out during a campaign of various finishing works. EDF took a number of additional measures to prevent these sleeves from misguidedly being blocked up again (by posting signs locally explaining the importance of the sleeves and also providing explanations in the CSS technical documentation).

In the context of startup tests on 1300 MWe reactors, a policy document was written by EDF to facilitate the detection and removal of loose parts. The document consisted of a cleaning test programme for systems not supplied by the main manufacturer of the reactor and some standard guidelines. EDF's concern was to determine for each system the possible points where foreign matter could accumulate. These points (around 400 in total) were made 'accessible' by installing orifices to accommodate examinations by endoscope.

The multi-hole diaphragm obstruction events affecting the safety injection system of the 1300 MWe reactors at the Saint-Alban and Flamanville nuclear power plants raised questions about the need for this type of diaphragm (compared to the single-hole flow-limiting diaphragms installed in 900 MWe reactors) and how to avoid the recurrence of these events. Similarly, in July 1986, a loss of flow from a turbine-driven pump in the EFWS was observed at the Saint-Alban nuclear power plant during startup tests of Unit 2. The blockage was caused by the presence of rags in the pump. It was decided that measures should be taken at the design stage to minimize the risks associated with foreign matter (definition of requirements related to pipes, tanks and sumps, installation of plugs for endoscopic examinations, installation of filters, etc.).

One particular issue is the cleaning of equipment that uses auxiliary fluids. Several events have occurred, including the following at 1300 MWe reactors:

- delivery of contaminated fuel oil to the storage tanks,
- seizing on diesel generator injection pumps (fuel oil not properly filtered),
- seizing on solenoid valves in the air-start system for starting the diesel generators (air not properly filtered),
- cases of contamination of the safety injection pump oil by water in the vent and drain system (design defect),
- damage to diesel generator turbochargers due to the presence of concrete residues in the air suction pipes to the motor intake system (pipe design),
- poor venting of the lines controlling the reactor coolant system protection valves (water not deaerated),
- seizing on emergency feedwater supply pumps (insufficient clearance),
- leakage on the check valves of the emergency-supplied instrument compressed air system (SAR).

Similar problems were encountered with the N4 reactor series, particularly those at the Civaux nuclear power plant:

- seizing on diesel generator fuel injection pumps (fuel oil not properly filtered),
- delivery of contaminated fuel oil to the storage tanks,
- seizing on the emergency feedwater supply pumps due to particles in the incoming fluid,
- seizing on the pumps supplying fuel oil to the diesel generators due to the absence of filters.

With the N4 reactor series, further damage to the temporary filters installed for flushing tests was observed (in the FPCS, DEG, CSS systems[626], etc.), along with the presence of foreign matter (for example, in the backup turbine-driven pump of the EFWS). This prompted EDF to mechanically reinforce these filters and install a differential pressure sensor on the sleeves of these temporary filters to monitor clogging. Contamination of the systems controlling the pressurizer's SEBIM™ valves[627] was also the cause of malfunctions on these valves, which led to the installation of filters.

These problems stem from insufficient information in the definition of the requirements associated with the auxiliary fluids used for equipment important to safety. Contamination of these systems has been found on all plant units. It is caused by deficient cleaning of system lines and inefficient filtration devices (worn or missing filters).

[626] The FPCS is the system that treats and cools the water in the reactor cavity and the spent fuel pool, the DEG is the chilled water distribution system, and the CSS is the containment spray system.

[627] The systems that control these valves, using the water in the reactor coolant system, have valves with a very small cross-sectional flow area.

In the case of the reactor coolant system, one event was of particular importance: at Unit 1 of the Paluel nuclear power plant, the presence of a metal brush during the hot tests, which led to the dispersal of more than 1500 bristles. A major programme was necessary to locate all this foreign matter. In some cases, the bristles had become embedded several millimetres deep in rod cluster control assembly guide tubes, which had to be replaced. This dispersal was aggravated by the fact that, for this first-off plant unit, the reactor internals instrumentation prevented the installation of filter blocks during hot tests.

In addition, loose parts have also been produced by deterioration of the filter blocks installed during hot tests:

- in Unit 2 at the Paluel nuclear power plant, more than half of the filter blocks installed during hot tests showed signs of deterioration, which meant that similar searches to the ones described above had to be carried out;
- in Unit B2 at the Chooz nuclear power plant, a piece of a filter block screen was found in a steam generator channel head;
- in Unit 1 at the Civaux nuclear power plant, several items were found when the lower internals were removed (two sheared rods, four pieces of screen);
- in Unit 2 at the same nuclear power plant, hot tests were stopped when loose parts were detected in a steam generator channel head by the vibration and acoustic monitoring system (KIR). Three broken tie-bolts were found to be present in the reactor vessel along with pieces of a fourth in the steam generator channel head, which was damaged. Five fuel assembly grids were also damaged.

These events required large-scale investigations (inspection of the reactor vessel and systems, passing felt plugs through the steam generator tube bundles, etc.), and repair of the damaged channel head.

A significant contamination event affected the fuel in Unit1 of the Chooz B nuclear power plant during the startup test phase in April 1995. Because a rainwater downpipe had become blocked, cleaning of the fuel building roof had caused dirty water to overflow, running along the walls and the overhead crane brackets and contaminating the spent fuel pool and the fuel transfer compartment. This contamination meant that a large number of operations had to be carried out:

- repairing the cranes and cleaning the structural framework,
- having the pool cleaned by divers,
- washing the fuel assemblies (for each assembly, individual rinsing and internal cleaning by extracting the rod cluster control assembly and vacuum-cleaning the guide tubes).

Another observation revealed that the elimination of best practices (flushing the steam generators after starting up the feedwater plant in the turbine hall) at the Nogent-sur-Seine nuclear power plant led to sludge formation at the bottom of the steam generators. The hardening of this sludge and the resulting stress occurring at the end of an operating cycle caused damage to the steam generator tubes, which was discovered in 1989 during the first refuelling outage of Unit 1. EDF subsequently prepared and implemented a procedure to check the cleaning of steam generators following testing of major transients, so that the first reactor operating cycle could begin with clean steam generators.

19.4.7. Piping support structures and displacement

The test programme for piping includes checks and measurements to be performed to inspect the support structures and check displacement of pipes in the reactor coolant system, secondary cooling system and auxiliary systems, and ensure that insulation is capable of fulfilling its function. Inspections carried out before the hot tests involve checking devices such as spring-hanger casings and self-locking devices, and checking clearance on stops and guides, as well as between pipes and self-locking systems.

Displacement checks during hot testing and power escalation on a pressurized water reactor are carried out on pipes in which temperature causes significant displacement or for which anchors to other lines (mainly the main primary system) are subject to significant displacement. They concern the portions of systems where temperatures rise above 100°C during operation, and portions of system lines in which fluids do not circulate, between the reactor coolant system and a 'fixed point' of the facility. As regards the reactor coolant system, the clearances obtained after adjustment and insertion of spacers are checked again after the second thermal cycling during pre-critical hot tests. Because these checks are only carried out on systems supplied by Framatome, the safety organizations asked EDF to extend the checks, defining their scope (identification of systems or parts of systems) and the checking success criteria.

19.4.8. Pump and piping vibrations

Piping vibrations are caused either by rotating machines or by hydraulic phenomena in the pipes themselves. In the case of rotating machines, the vibration levels are measured at startup and periodically throughout the facility lifetime. An analysis of the test programmes for 1300 MWe reactors showed that the operator had not systematically planned to take these measurements across the entire speed range of the rotating machines. In addition, the criteria used at startup and during operation to decide on the acceptability of vibration levels were the focus of discussions between EDF and the safety organizations.

In the case of piping vibrations, no systematic checks were carried out at the time except for certain measurements on well identified parts of the reactor coolant system and on the reactor internals for the first-off plant units. Vibrations can eventually cause pipes to crack or even rupture, generally at branch connections, causing a wide variety of consequences ranging from a simple leak to the unavailability of valves, pumps or even entire loops. Staying with French experience in this area, the most significant event because of its scale is probably the one that occurred in August 1978 affecting the main steam bypass to condenser (MSBc) in Unit 2 at the Bugey nuclear power plant (a 900 MWe reactor in the CP0 group), in which cracks were found in pipes downstream of valves, at welds where they were connected to the main piping. The damage found was explained by the amplitudes and accelerations associated with vibrations measured after the event. The event led to a design review of the MSBc in the facility's four units and led to partial unavailability of the main steam bypass to the condenser, required for use in some transients.

Other events caused by vibrations on 900 MWe reactors include:

- breaks in air supply lines to the flow control valves in the residual heat removal system, in main steam isolation valves (Fessenheim, Bugey) and in steam generator feedwater valves (at Gravelines),
- repeated damage to temperature sensors in the reactor protection system on the reactor coolant loop bypasses during pre-critical hot tests (Unit 2 at the Le Blayais nuclear power plant),
- damage to the supports of the pressurizer relief line following repeated stress on the relief valves (at Dampierre-en-Burly),
- breaks in the minimum flow lines[628] of demineralized water pumps (Unit B2 at the Chinon nuclear power plant).

These events, given as an example, are not an exhaustive survey of damage caused by vibrations. Their only consequence was reactor unavailability and the review of measures adopted during design studies. Operating experience based on events caused by vibrations or on pipe inspection findings should provide a better understanding of the problems likely to arise at sensitive points of systems during operation and should make it possible to correct any defects or provide special monitoring. However, the safety organizations considered that it was better for this to be done at the time of startup tests and for measures to be taken without waiting for further events to occur; in any case, using the startup tests to check that the sensitive points of systems could not cause problems seemed imperative in the case of the engineered safety systems, which would not benefit from operating experience feedback. Most accident configurations are only tested in the startup phase and are not reproduced later on during periodic tests. EDF was therefore asked to establish a vibration measurement programme for the sensitive points in systems, particularly engineered safety systems, taking into account their different operating configurations. This programme was to be included in the general framework of startup tests and would check that pipework had been correctly installed. EDF was invited to draw inspiration from programmes recommended or applied at the time to nuclear power plants in other countries, in accordance with the requirements in the U.S. NRC Regulatory Guide RG.1.68.

A large number of anomalies were found on 1300 MWe reactors, including:

- ruptures of reactor coolant system temperature sensors,
- erosion of some (gas or steam) letdown orifices,

[628] Lines guaranteeing a minimum flow to a pump when it is in operation.

- pipe connection ruptures,
- cavitation in certain valves.

These anomalies were due to shortcomings in system design studies. In particular, no checks were carried out on any of the flow restrictors in any operating configuration, to ensure the conditions for avoiding cavitation were met. In addition, there was no exhaustive list of sources of vibrational excitation and no checks were carried out to ensure the relevant equipment was well-adapted for its purpose (identification of natural frequencies, vibration measurements at branch connections, etc.). The specific case of stresses resulting from the opening of protection valves was not explicitly taken into account.

With the N4 series, damage to pipe connections was observed again during tests on Unit 1 at the Chooz B nuclear power plant. EDF took into account this operating experience feedback by making design changes (installation of reinforced sleeves on pipe connections considered to be sensitive, geometry changes, elimination of some fixed points, etc.). More generally, at all reactors EDF deployed a method of identifying sensitive pipe connections and took vibration measurements, particularly on engineered safety systems and the associated support systems, in all configurations (normal operation, accident situations, periodic test configurations, etc.). Tests were performed for this purpose on Unit 2 at the Chooz B nuclear power plant. The findings led to corrective action (modification of supports, changes to the type of diaphragm, etc.). Endurance tests were carried out on some machines to check the strength of instrumentation taps, vents and bleed valves (liquid penetrant testing).

19.4.9. Validation of operating procedures and periodic tests

During the startup tests, normal operating procedures are used extensively, which means they can be validated. Incident and emergency procedures, including H and U procedures, are validated where possible on one reactor in the series. In all cases, the procedures are validated on a simulator or using simulation software.

One of the objectives of the startup tests is to allow operating crews to familiarize themselves with the facility. The startup phase includes validation of operating documents and periodic test documents.

Following startup of reactors in the 900 MWe and 1300 MWe series, and as a result of comments made by safety organizations, EDF improved the procedure for achieving this objective by making it more explicit. The documentation associated with the tests was supplemented to make the validation process more exhaustive and ensure traceability of the results after the tests had been performed. These improvements were beneficial during the startup tests on the N4 reactor series.

The normal operating procedures (referred to as ‘F’ and ‘G’) are validated by the operator in collaboration with the build contractor. After analysis, the build contractor incorporates all the comments and produces a procedure with a higher revision number. When the 900 MWe reactors were started up, validation reports did not exist and therefore were not reviewed by safety organizations. Experience with starting up the 900 MWe units under the CPY programme contracts showed that, in some cases, anomalies important to safety were discovered during these validations. For example, during thermal conditioning[629] of the reactor's residual heat removal system (RHRS), because the flow rate allowed into the system was at least 200 m^3/h (value imposed by a mechanical stop on the flow regulation valve in the heat exchangers), a warm front moved through the system, placing stress on the docking flanges of the RHRS pumps to the extent that the operators noticed leakage. A new procedure was developed for this series so that the RHRS could be thermally conditioned with the pumps shut down, minimizing thermal shocks. It was better for this type of malfunction to be reported without delay to the safety organizations. Accordingly, EDF was asked to present any major problems or anomalies detected during use of normal operating procedures, at meetings of the on-site test committees.

As stated earlier, the test working group set up for startup of the 900 MWe reactors pointed out that the guarantee of facility compliance was based in large part on conducting periodic tests, which at the time only started after core loading. For some systems, depending on the difficulties encountered on the construction site, a year or more could elapse between the functional system tests and core loading. During this time, there could be significant activity in the vicinity of a system and there was no guarantee that, even if it had been operational at the time of functional testing, it would still be so when the core was loaded. For systems and equipment subject to monthly testing, this was not a particularly serious issue, but for systems and equipment tested only at the time of refuelling (such as the containment isolation system), the consequences could be more serious. As a result, the group decided that periodic tests for refuelling should be carried out for the first time before the first fuelling. This requirement was continued for subsequent reactor series.

19.4.10. Uncertainty and 'set points'

Reactor protection system set point values, i.e. the threshold values of a certain number of reactor operating parameters which, if reached, trigger the protection system, are calculated to mitigate the risks of the incidents and accidents included in the deterministic safety analysis (see Section 5.6). Safety analysis reports present the threshold values that trigger a reactor trip. These values differ from the threshold values set in the facility itself, the difference being the sum of the uncertainties related respectively to the accuracy of the measurement electronics and the accuracy of the triggering device. The appropriateness of the set point values must be demonstrated by the operator. In the case of testing, checks carried out in the facility must show that, taking into account the accuracy of the installed equipment, the trigger thresholds during operation are compatible with the values substantiated in the deterministic safety analysis.

[629] Gradual increase in temperature performed prior to commissioning at nominal temperature.

When a reactor is first started up, measurements must be taken to calibrate protective devices. For these measurements to be taken, the reactor must be operated at power, but it must be certain that, while at power, the protection system remains capable of performing its function if an incident or accident occurs. This dilemma is resolved by setting very conservative protection threshold values when the reactor is operating at low power so that low-power tests can be performed. Based on the results, it can be shown that slightly less conservative thresholds could be used for the next power level.

Despite the formal procedures and all the precautions taken during startup, one 900 MWe unit still operated (for a limited time) with an incorrectly calibrated protection system (error of a factor of two in the non-conservative direction for the axial neutron flux imbalance – see Section 5.2). To detect this type of malfunction in time, it is necessary throughout power escalation to determine the margins between the operating point and the protection trigger point for stable reactor situations; it is then possible to detect any operating errors, by comparison with readings taken during power escalations of reactors started up previously.

On this subject, recommendations and requests have been made by the safety organizations to further improve the accuracy of set point adjustment operations during reactor power escalations and the traceability of information provided to demonstrate the conservatism of set point values.

19.4.11. Condition of facilities during startup tests

The main purpose of startup tests is to check that facilities comply with the design studies and the corresponding safety demonstration. EDF has made significant efforts over time to define these tests. However, it is important to remember that the aim is to ensure facility compliance not just during startup tests, but also during reactor operation.

If the success of a test was limited to a comparison of a numerical result with a criterion, this would only guarantee compliance at the time of testing. Containment strength tests and leak tests can provide a simple illustration of this. Essentially, there are two ways of measuring the total leak rate of a nuclear power reactor containment. In the first case, the test is scheduled very early in the construction schedule when certain containment penetrations have not yet been fitted with their final isolation devices and are simply plugged. In this case the leak rate measurement process is completed later on by measuring the leak rates from each of these penetrations once they are fitted with their final isolation devices. In the second case, the test is scheduled after the hot tests, once the containment is in its final configuration and the total leak rate is obtained by a single measurement. Mathematically, the result may be the same as regards the total leak rate from the containment, but the second method is far preferable in terms of representativeness of the reactor state and compliance with requirements before the first core loading. This example shows that it can be important to consider which state of the equipment and which environment are the most pertinent for test purposes.

In the case of instrumentation and control systems, checks are carried out during the first tests of each system by setting instrumentation chains into operation and checking that actuators function correctly. However, work or changes carried out at a later time can affect continuity or the hardwired routing of instrumentation and control signals. In this case, functional testing of automatic actions implemented for incident or accident situations is necessary during the integrated system tests carried out during startup testing. If possible, this should be done in the final phase, unless temporary measures and devices have to be installed that would significantly affect test representativeness or that would involve an excessive risk of the configuration being incorrectly restored, which would be undetectable later on and would pose a safety risk.

It is advantageous to test equipment as early as possible to detect any major malfunctions. However, for integrated system tests to be representative of reactor operation after core loading, the minimum level of readiness of the system and its environment before the integrated system tests begin needs to be determined so as to minimize work after the test period. For the phase after the first core loading, EDF adopted a useful rule requiring an advanced level of readiness in order to perform tests: testing can only be conducted once the buildings located in a ‘controlled area’ (in the radiation protection sense) during normal operation are effectively placed in an operational controlled area context. Experience of reactor startups has also shown that changes are still necessary after the integrated system tests; facility compliance therefore depends on the organization set up to manage these changes and any associated requalification tests.

19.4.12. Other aspects

As will be explained in Section 19.5, IPSN had cause to recommend that EDF carry out end-of-assembly tests on passive equipment[630] such as containment sump filters, in addition to its planned startup tests. The end-of-assembly tests on sump filters did not include checking that there were no gaps larger than the filter mesh, which could lead to the risk of filter bypass. In view of the tests on the Flamanville 3 EPR, EDF carried out a more general analysis of the inspections and tests to be performed on passive equipment items (excluding civil works) that do not belong to an elementary plant system. This analysis sets out the design requirements adopted for each postulated phenomenon (flooding, fire, contamination, etc.) and each equipment family, and the inspections and tests to be performed to check that these requirements have been met. For civil works, all the necessary inspections and tests are carried out during construction, except for leak tests on the pools and containment.

Beginning with startup tests on 1450 MWe reactors (N4 series), a final compliance review was carried out on certain cross-functional equipment items produced by several different entities (different contracts or trades) or that underwent several changes related to the activities and work being carried out at the facility. The checks

[630] Passive equipment important to protection is equipment that does not need to change state to perform its function (accumulator, pipe, pipe support, etc.).

carried out for this review involved, for example, making sure that redundant trains were physically independent, checking fire compartmentation, checking for any risk of damage to equipment important to safety in an earthquake by equipment not designed for earthquake conditions, or checking measures to protect against external flooding.

It is important that design choices ensure that startup tests (and later on, periodic tests) can be performed under the correct conditions, for example, without causing a risk of corrosion on metal components or structures.

Finally, general operating experience obtained over time from the startup and operation of French nuclear power reactors has led to further tests being added to the startup test programmes. Where these were not carried out on a reactor initially, they have been carried out during the ten-yearly reactor outages of that reactor. One example of this is blowdown testing conducted on safety injection system accumulators.

19.5. Examples of findings resulting from startup tests

Some of the findings of startup tests conducted on reactors in the nuclear power plant fleet provide a concrete illustration of some of the aspects mentioned above, particularly concerning the safety functions for which representative integrated system tests cannot be carried out on site, such as safety injection or water circulation in the containment in accident conditions.

Subsequent to startup tests, two other observations were made during reactor operation following the installation of new equipment, where the lessons learned are relevant to startup tests in general. These findings involved anomalies observed in the device that measures the water level in the vessel, installed during deployment of the 'state-oriented approach' for incident or accident operational tasks, as well as instances of noncompliance observed on diaphragms in the filtered venting system associated with the U5 accident procedure, installed in reactors as part of measures to mitigate the radiological risks of core-melt situations.

▶ Bypass of the containment sump filters in accident conditions

On 1300 MWe reactors, the water collected in the containment sumps is filtered in several stages. The finest filtration mesh is 2.5 mm, defined to prevent local clogging in the fuel assembly grids, partial clogging of the multi-hole diaphragms in the LHSI or the CSS spray nozzles in the containment, clogging of the CSS heat exchangers or damage to the SIS or CSS pumps. The filter panels are vertical and provide three successive filtration stages with 30 mm × 30 mm, 10 mm × 10 mm and finally 2.5 mm × 2.5 mm meshes.

In December 1989, while monitoring the startup tests on Unit 1 at the Golfech nuclear power plant, IPSN noticed an installation anomaly that could lead to bypassing the sump filters. The size of the holes in the upper plates for the two water-level measuring devices in these sumps were such that the filters could be bypassed, with a 5 cm gap being the smallest-sized hole (see Figure 19.3).

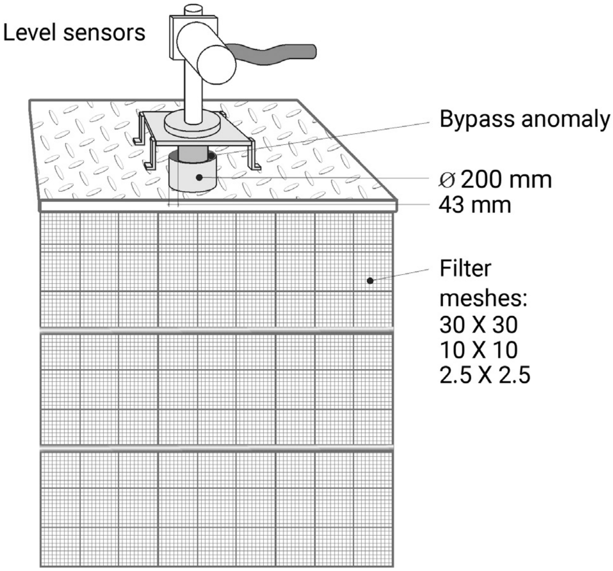


Figure 19.3. Containment sump filter anomaly at Golfech Unit 1. IRSN.

If there was a reactor coolant system break, the two trains of the safety injection system and containment spray system, and therefore the corresponding functions, would have been lost because of this filter bypass. EDF therefore:

- made a change before the unit went critical,
- assessed the situation on other reactors (900 MWe and 1300 MWe units),
- specified the subsequent actions that would be taken,
- identified the source of the anomaly.

EDF very quickly made changes on Unit 1 at the Golfech nuclear power plant and on Unit 1 at the Penly nuclear power plant, before they went critical. However, checks showed that other reactors were affected by the same or similar anomalies. More specifically, all the 1300 MWe reactors were affected, with several types of anomaly: excessively large holes for measuring devices, excessively large gaps between filters and concrete structures, pin holes that had not been replugged, etc. Only six of the 900 MWe reactors were not affected by anomalies; however, these anomalies were smaller than those found on the 1300 MWe reactors, the maximum observed clearance being 7 mm.

In terms of general lessons learned, these anomalies showed that:

- the safety measures initially adopted at the design stage had been forgotten when the sumps and associated equipment were installed on site,
- the quality assurance level of the assembly operations was not in agreement with the sump filter safety classification,
- installation and checks had been carried out without the required precision.

Because these anomalies on approximately 40 reactors had involved several build contractors, they cast doubt on the 'quality organization' of EDF's Equipment Branch. Other similar anomalies were found at the same time, affecting the diaphragms in containment filtered venting systems (see below). This series of quality defects prompted EDF's Equipment Branch to set up a working group in 1990 to investigate in detail the causes of these defects and the reasons why they were not detected or corrected satisfactorily. The aim of this investigation was to define concrete improvement measures, wherever possible with measurable effects, that would reduce the risks of anomalies and eliminate significant malfunctions. The subjects to be covered were:

- the internal organization of studies, work and verifications at the Equipment Branch, and improvement of the corresponding interfaces,
- the procedures for qualifying systems and functions where qualification cannot be achieved by testing.

In addition, and more generally, these anomalies caused EDF to conduct a study on safety measures that cannot be checked by testing, which led to the introduction of additional periodic tests, some of them to be applied retroactively.

▶ Excessive vibration and rotor lift in SIS and CSS pumps

The SIS and CSS systems both have motor-driven pumps with vertical shafts, as shown in Figure 19.4. The motor and the pump are installed on two different levels about 4 m apart, with a vertical splined sliding transmission shaft fitted with universal joints that is 2.6 m long.

The anomalies discussed here concern the low-head safety injection (LHSI) pumps and the containment spray system (CSS) pumps in 900 MWe reactors and P4 1300 MWe reactors.

After detection of vibrations exceeding the admissible value when a CSS pump was started up on Unit 1 at the Paluel nuclear power plant (a P4 1300 MWe reactor), a 2000-hour endurance test was carried out from January to July 1985 on the CSS pumps on Unit 2 at the Saint-Alban nuclear power plant. This test aimed to demonstrate that the robustness of the moving parts in these pumps would allow them to withstand high vibration levels without rapid damage. In order to produce these vibration levels, an unbalanced condition was created by installing an eccentric steel plate. The test confirmed the robustness of the moving parts, but revealed another phenomenon that threatened pump reliability. It appeared that the expansion of the pump body when it took in hot water caused the rotor on the electric motor to lift. In the event of a loss-of coolant-accident, the water in the sumps can be taken in by suction from the SIS and CSS pumps when the water is at temperatures reaching 120°C.

Analysis attributed the anomaly to the design of the rotating parts on the CSS pumps, which included a 'single-acting' upper bearing taking up only the weight of the rotor. It also raised questions about the possibility of similar anomalies on other vertical-shaft pumps, particularly the low-head safety injection (LHSI) pumps. To correct these anomalies,

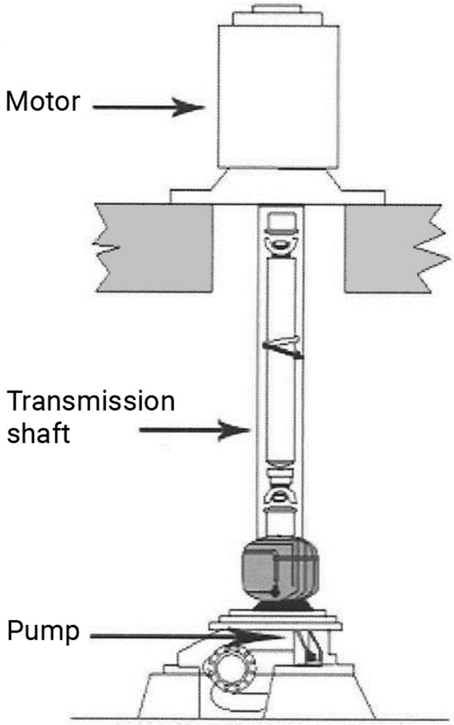


Figure 19.4. Diagram of the vertical-shaft pumps in the SIS and CSS systems. IRSN.

EDF decided to fit all the motors on the relevant pumps on 1300 MWe reactors with a ‘double-acting’ upper bearing, i.e. one that would take the downward and upward loads.

In the case of 900 MWe reactors, operating tests were carried out in 1992 on the low-head safety injection system pumps on Unit 2 at the Fessenheim nuclear power plant (CP0), at the time of its first periodic review. The duration of these tests had to be longer than that of the periodic tests (30 min). After giving the pumps 5 h to reach thermal equilibrium, the tests revealed vibrations of greater amplitude than the amplitude at which they should be shut down (this time period explains why these vibrations were not observed during periodic tests).

Modifications were then also made to these pumps. In particular it became apparent that the natural frequency of the transmission shafts was too similar to the rotation speed of the motors (1500 rpm, or 25 Hz); they were replaced and their tilt angle was reduced to diminish the associated vibratory excitation. Sliding was also improved by adding a special coating to the splines to reduce friction, after blocking had been observed several times, and grease fittings were also added. Finally, tie rods (stays) were installed between the fixed parts of the motors and the support bases to increase the difference between the motors’ natural frequency and rotation speed. Later on, a similar modification to the one mentioned above for 1300 MWe reactors (installation of a ‘double-acting’ upper bearing) was made to 900 MWe reactors (2006).

The fact that the vibration anomalies were only identified during long-term tests on engineered safety pumps underlines the problem of the representativeness of startup tests (or periodic tests), which are not always able to explore all the unfavourable conditions that equipment may be subject to, particularly in accident situations; the temperature of the water drawn into the sump probably did not exceed 80°C during the endurance test at Saint-Alban.

It has generally seemed necessary for EDF to analyse all anomalies appearing during startup tests by performing tests, measurements and studies in addition to the qualification tests and first-off plant unit tests. This is why, in June 1989, the Central Service for the Safety of Nuclear Installations asked EDF, in the case of engineered safety pumps not continuously in operation during normal operation, to investigate the possibility of performing tests that represented operating conditions for a significant duration on site, for all first-off plant unit equipment. EDF therefore performed long-term on-site tests of up to 8000 h on LHSI and CSS pumps. Based on the results, EDF considered that it was not necessary to carry out further long-term tests in addition to the 400-hour endurance tests required for qualification of the equipment mock-up and the 20-hour tests for series-produced equipment (these shorter tests are performed at the factory). It believed that the endurance test, together with a detailed expert assessment, was enough to detect any physical phenomena that might affect pump operability. However, it seemed necessary, among other lessons learned, for the reference vibration level of each pump to be determined from the results of the endurance tests and on-site tests.

The tests planned by EDF nevertheless continued to reveal vibration anomalies in engineered safety system pumps, particularly those of the 900 MWe units under the CPY programme contracts; this will be discussed further in Section 29.2.2.9.

As indicated in Section 19.4.2, in view of the lessons learned from the observations described above, EDF carried out 1500-hour tests of the SIS and CSS pumps on the first units in the N4 series; apart from a few adjustments[631], these pumps have not revealed any significant malfunctions. The case of the Flamanville 3 EPR was also mentioned in Section 19.4.2.

▶ Issues with control of motorized valves in the safety injection system

In November 1986, an apparently minor incident that occurred during pre-operational testing of the first unit at the Nogent-sur-Seine nuclear power plant led to the discovery, following analysis of the incident, of a generic anomaly affecting the safety injection system on 1300 MWe reactors; this anomaly could have seriously compromised the operation of the safety injection system in the event of a reactor coolant system break.

[631] To the medium-head safety injection pumps: modification of the impeller and volute geometry, sharpening of the vanes.

The event consisted of problems in operating the safety injection system motorized valves. These problems mainly affected the minimum flow isolation valves of the LHSI pumps to the FPCS tank. When the tests were resumed in February 1987 after various interventions, the valves continued to operate incorrectly.

Further investigations on units at the Belleville-sur-Loire and Cattenom nuclear power plants revealed the same type of problem. Sizing of the valves, drive systems and transmission devices was thought to be the problem. It emerged that changes to the design of the safety injection system were not reflected in the valve control devices and that undersized equipment had been installed. The generic nature of the anomaly was then confirmed; nearly 70 valves were affected at all the 1300 MWe reactors (types P4 and P'4).

It is important to note that undersizing of the drive systems was only detected at startup during testing of the eleventh 1300 MWe reactor, i.e. after about four years of operating the first 1300 MWe reactors. The reason why the problem was discovered by chance is partly explained by the fact that incomplete closure of the valves could only be detected locally.

Other events were then observed affecting motorized valves in the safety injection systems at the Nogent-sur-Seine, Penly and Golfech nuclear power plants, with ruptures of universal joints in the remote-control systems of these valves.

EDF took measures to bring the remote-control devices on these valves into compliance and to ensure design changes would subsequently be reported in change notices sent to all the relevant departments (including those responsible for ordering equipment) so the impact of the changes could be checked. It also took steps to improve quality assurance in design work and equipment installation on site.

These anomalies caused IPSN to take a close look at a certain number of aspects involved in sizing motorized valve drive systems, taking into account all the configurations in which they may be found during testing and operation in normal, incident and accident situations. This analysis showed that, in general, the test instruments used on the valves during the reactor startup tests and during operation could not detect all the different types of valve damage that could lead to failure. Various systems offering better performance were studied and deployed on reactors in service to improve the situation.

No anomalies had been detected during the qualification tests of the loop valves because the flow rate in the test loops was insufficient.

▶ Inversion of electrical control cables of effluent reinjection pumps in the reactor building

Effluent reinjection into the reactor building, a function introduced following the Three Mile Island accident, aims to control the spread of contamination to the auxiliary buildings (NAB, SAB, FB, ETB)[632] from the reactor building in the event of leakage from the engineered safety systems as they recirculate water from the sumps. If a channel of the plant radiation monitoring system (PRMS) detects an activity concentration above a set threshold in a sump in one of the auxiliary buildings, an automated system stops the relevant sump pump and closes the valve on the line that connects to the effluent treatment building. In accordance with instructions in the U2 accident procedure (see Section 17.5.2), the operator performs a radioactive effluent reinjection into the reactor building by opening the valve of the reinjection system in that building and starting the relevant sump pump.

An anomaly affecting effluent reinjection was discovered by chance in June 1990 during the startup tests on Unit 1 at the Golfech nuclear power plant. It emerged during these tests that, in the case of eight of the ten monitoring channels, the automated system did not start the relevant sump pump, but the pump of a neighbouring sump. All the documents (elementary system files, test procedures, periodic test procedures) for the systems concerned and the U2 ultimate emergency operating procedure contained these inversions.

It also emerged that the anomaly only affected the type P'4 1300 MWe reactors and was the result of a discrepancy between two elementary system files produced by different people. Corrective measures were defined and implemented (changes in the CONTROBLOC computerized relay racks), and the operational and design documentation was also updated.

A review of plans to check the consistency of the PRMS with other systems also revealed other anomalies: inversion of the intake pipes of PRMS channels in ventilation systems (in the nuclear auxiliary building [DVQ] and the effluent treatment building [DVN]).

EDF learned the following lessons from these anomalies: that particular care must be taken with identical elements belonging to the same train; and that the boundaries between the PRMS and other systems can be a source of errors. In the case of the N4 series, this source of errors was eliminated by incorporating all the elements of the PRMS channels into the 'user' elementary plant systems, thus removing the interface problem. Further checks were also carried out on the whole nuclear power plant fleet.

In IPSN's view, the late chance discovery of the anomalies was due primarily to the inadequate representativeness of the testing carried out (during startup tests and periodic tests) on the automated systems actuated by the PRMS, from detection of the physical phenomenon to the required actions being taken. The anomalies might have been detected sooner if a radioactive source had been placed in front of the monitoring devices during testing. This type of test would have also revealed the inversion of two sampling input pipes on a PRMS cabinet, discovered by chance at Golfech and due to an installation error.

[632] Nuclear Auxiliary Building, Safeguard Auxiliary Building, Fuel Building, Effluent Treatment Building.

For reactors in operation, EDF was asked to conduct tests on the PRMS automated system channels using radioactive sources, except in exceptional cases where the activity of the necessary source would be too high. During startup tests on the N4 reactor series, IPSN very carefully monitored scheduling of this type of test on all reactors.

Concerning the inspection and testing of identical elements belonging to the same channel, IPSN carried out a specific analysis in the case of fire detectors (JDT system). This analysis showed that the test documents did not, as written, rule out the risks of addressing errors on detectors using a certain technology. Because an addressing error between two channels of the JDT system, in the event of a fire affecting one of those channels, could cause the loss of the second by being switched off – something that might be decided to facilitate the response – EDF made changes to the test programme for this system.

▶ Anomalies related to reactor vessel water level measurement

Discussions in the wake of the Three Mile Island accident to improve operation in incident or accident situations prompted EDF to adopt the principle of operation based on the concept of reactor states. This is the 'state-oriented approach' (SOA) described in Chapter 33. The history of measuring the reactor vessel water level (sometimes referred to as the mass inventory) is closely linked to the history of SOA. SOA uses two key parameters: the subcooling margin and the reactor vessel water level. With SOA, operation is based on knowledge of the state of the reactor coolant system, the secondary cooling system, and the containment and systems used, rather than on determining the events that led to the situation in question.

At the beginning of 1982, EDF began the process of developing SOA and asked the build contractor Framatome (for the 900 MWe series) and EDF's engineering services (for the 1300 MWe series) for feasibility studies so that it could define the most appropriate device for reactor vessel water level measurement.

At the end of November 1982, the decision was made to equip 1300 MWe reactors with a device for measuring the water level based on differential pressure. Then, in 1984, the decision was made to replace 'event-oriented' procedures with SOA procedures. Once the necessary studies and modifications had been carried out, in 1990, Unit 1 at the Penly nuclear power plant was the first unit to be started up using this measuring device and the SOA procedures.

Clearly, the corresponding test programmes had to be examined very carefully. They were monitored very closely by IPSN, which recommended in particular that a validation test of the reactor vessel water level measuring device be carried out under real conditions with the creation of a steam bubble under the reactor vessel head. After a number of discussions about the risks associated with this kind of test (in particular on the ability of the reactor vessel head gasket to withstand the test), EDF performed a test in August 1989 in Unit 1 at Golfech nuclear power plant (during hot testing, without the core loaded). This test and the first test campaign run during hot tests of Unit 1 at the Penly nuclear power plant revealed various anomalies, in various reactor coolant system configurations and in the event of loss of electrical supply. Corrective actions, such as changes to the instrumentation and control software, were taken as a result.

This example emphasizes the importance of carrying out functional testing in conditions that are as close as possible to the real operating situations that can be envisaged.

▶ Noncompliant diaphragms in the containment venting system

As stated in Chapter 17, from 1987, following the Three Mile Island accident and on completion of various studies, EDF installed a U5 system in its reactors that would release controlled and filtered radioactive substances in the event of a core-melt accident in order to:

– limit pressure in the containment,

– reduce by at least a factor of 10 the radioactivity of aerosols released into the atmosphere,

– bring filtered gases to the nuclear auxiliary building (NAB) stack to measure their radioactivity before dispersion in the environment.

The plan was that this device would only be used after a delay of around 24 h, so that radioactivity could decay to a certain extent inside the containment.

To validate the installed devices, EDF proposed a programme of tests to be performed on the various reactors in the nuclear power plant fleet. Although this programme included partial tests of the device on site, it did not include a full integrated system test or flow rate measurement. All the planned tests were performed on all the sites in operation or in the startup phase. They included:

– testing the motorized valves for isolating containment penetrations,

– testing the pipes on the U5 system pressurized with air,

– testing the filter housing integrity.

Other tests were also carried out:

– a first-off plant unit test on Unit 2 at the Nogent-sur-Seine nuclear power plant, to measure velocity distribution inside the sand filter housing and the housing head-loss,

– for all reactors, a startup test on the conditioning (preheating) system in normal operation of the sand filter by diverting the ventilation provided by the DVN system.

During a test carried out at the initiative of the operator of the Tricastin nuclear power plant in August 1990, it became apparent that no hole had been drilled in the diaphragm in the containment venting pipe of Unit 1. Investigations subsequently carried out on all reactors revealed other anomalies: no diaphragm (only a spacer was present), incorrect drilling of the diaphragm (20 mm instead of 76 mm), diaphragm with no hole.

These diaphragm installation anomalies were only found by chance, despite inspections conducted at the time of fitting, verification and startup of facility operation. Documents and procedures existed to prevent these anomalies, but these documents were not always filled in properly and were not adequately checked. The elementary system file for the U5 system did not contain a technical data sheet for the diaphragm. Incomplete information given to those carrying out assembly operations and failure to listen to reservations made by various workers explain most of the anomalies found. The end-of-fabrication reports submitted by the assembly contractors appeared as formal documents that were too brief to fully describe the work performed and the difficulties encountered. In particular, these documents should have clearly stated the condition of the diaphragms and the hole diameters, and they should have been carefully reviewed by EDF on site to make sure they listed all the anomalies identified during installation.

As a result of these findings, EDF specified:

- the actions that it would take subsequently to ensure that the actuator and the characteristics of the flow-limiting orifices were formally checked at the time of on-site system acceptance to guarantee compliance with design specifications, and that any reservations would be followed up and checked before the first core loading or the next refuelling operation;
- the procedures to be followed to advance systems from the assembly phase to the test phase, so that the corresponding report certifies that the actuators and flow-limiting and measuring devices are compliant with the facility equipment management file[633] (or its equivalent) and that any remaining reservations are clearly identified.

IPSN had also recommended that EDF examine the possibility of carrying out a full test of the U5 system at the time of the containment building pressure test, temporarily installing a flow-limiting orifice and a HEPA filter in the containment to avoid contaminating the sand in the filters. For some reactors, EDF used the U5 system to vent the containment after its strength and leak tests, but this was later abandoned because of the disadvantages entailed:

- the need to fit a temporary valve for the test and then refit blind flanges,
- the need to provide a rupture disk to protect or bypass the filter for the periodic total leak test on the containment, which can constitute a weak point if used in an accident situation,
- the lack of accountability of any radioactive substances released when the containment is depressurized.

[633] File used for equipment management at nuclear power plants.

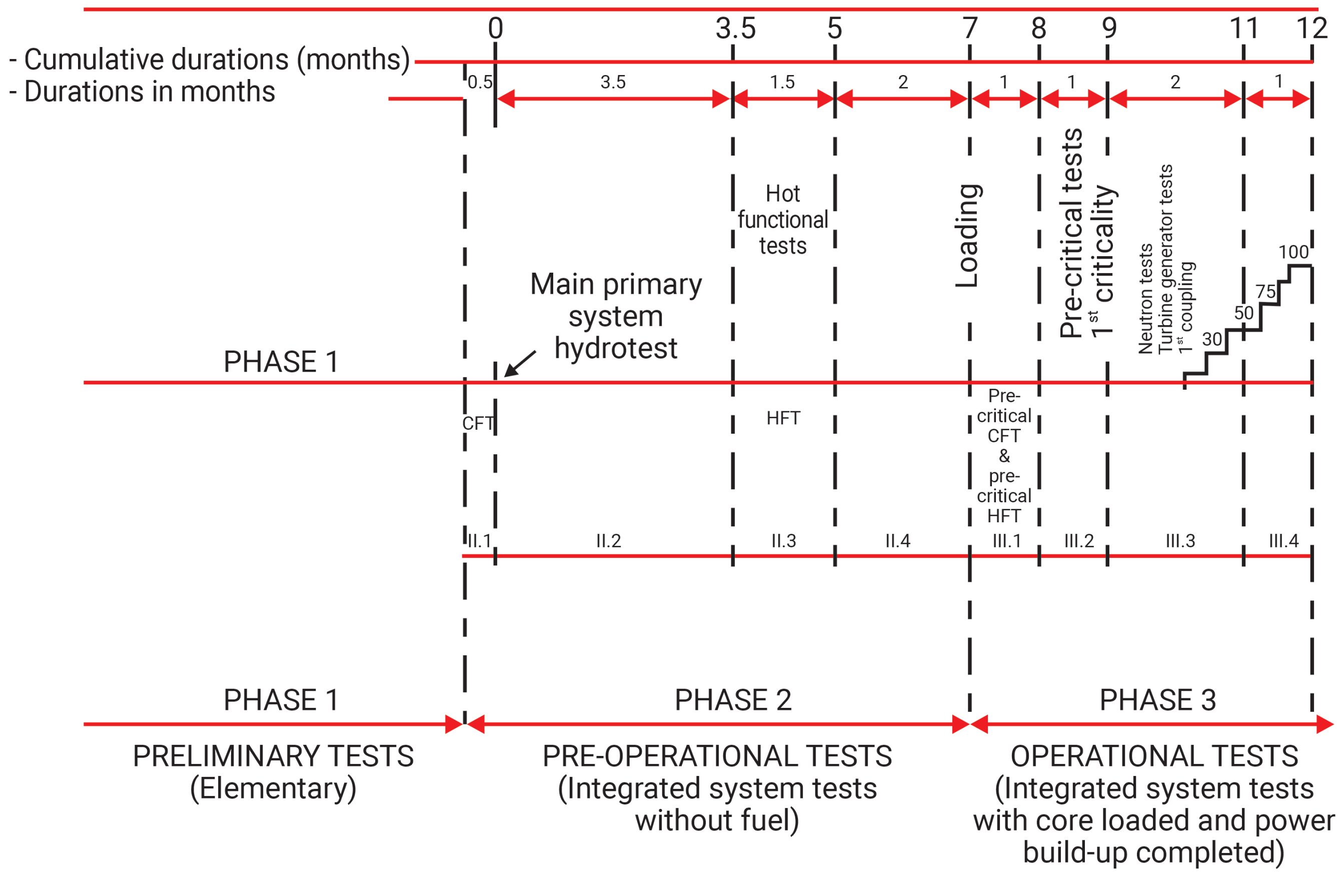


Plate 19.1. The different startup test phases.

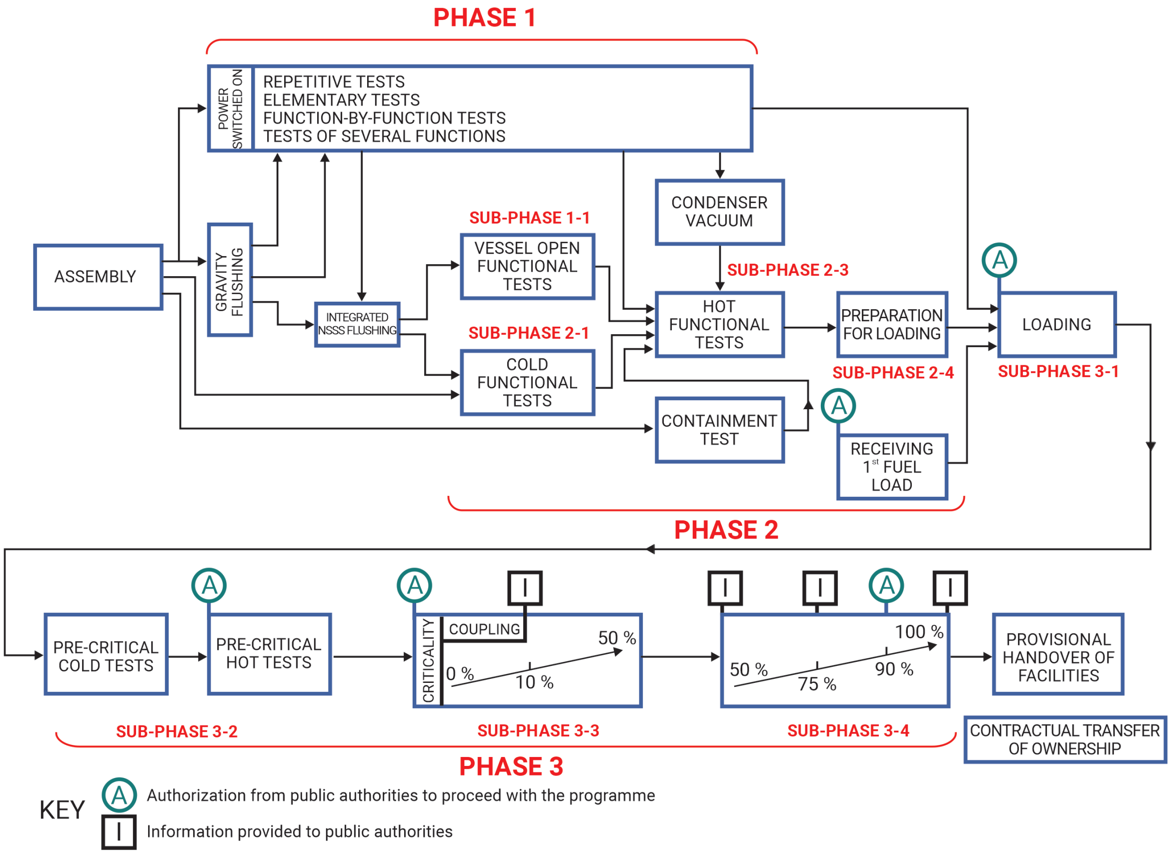


Plate 19.2. The different startup test phases.

Chapter 20
General Operating Rules

Facility design and construction play an essential role in preventing incidents and accidents, but taking into consideration operating conditions and constantly comparing what was planned at the design stage to what is achievable in daily operations represent another essential aspect of nuclear safety.

Nuclear safety organizations thus closely examine everything involved in operation, which, as for design and construction, in no way exempts facility operators from their responsibilities. The operator must:

- prevent incidents by maintaining facility safety at the level set in the design phase, notably by:
    - complying with 'Operational Limits and Conditions' in all operational activities,
    - maintaining and checking the availability and reliability of equipment important to safety, by:
        - performing periodic tests,
        - performing preventive or curative maintenance on equipment (a subject covered in Chapter 26),
        - requalifying this equipment after maintenance;
- manage any incidents and accidents under conditions compliant with design assumptions, by:

    - detecting any deviations in operating conditions compared to the authorized domain,
    - establishing and using incident and accident operating procedures and preparing for the management of core-melt situations,
    - using the on-site emergency plan that ensures appropriate internal organization and interfaces between the facility and outside responders as soon as the situation shows signs of an upset;
- seek to improve the effective level of safety:
    - by correcting any weak points in design, construction or operation brought to light by experience or any other safety studies,
    - by considering changes in safety objectives over time and the requirements set out by the French Nuclear Safety Authority (ASN),
    - by disseminating good operating practices.

20.1. General Operating Rules

The safety studies conducted at the design stage of a facility or as part of periodic reviews define technical and organizational measures to ensure safe operation of the facility. However, they cannot be used directly in everyday operations. They must be translated into a more operational form that can serve as a reference to operating personnel who are involved in facility operation as well as control and maintenance activities.

The 'General Operating Rules' make this transposition possible and provide a link to documents that can be used directly in operations.

During design and construction of the first units of the French nuclear power plant fleet, general operating rules were part of the 'intermediate safety analysis reports' and then the 'final safety analysis reports'. In 1973, the decision was made to use them to prepare a separate document, easier to manage and update than the safety analysis reports. The construction authorization decrees for the various 900 MWe, 1300 MWe, and 1450 MWe units stipulated that general operating rule proposals were to accompany, first, the intermediate, then the final safety analysis reports, and that they were to be approved by the relevant minister(s) during the fuel loading permit application and then the operating authorization application, pursuant to Decree 63-1228 of 11 December 1963 as amended, concerning (basic) nuclear installations. In the modifications made to this decree, it was stipulated that the first general operating rule proposals had to be submitted at least six months before the first reactor fuel loading operation. This decree was repealed by Decree 2007-1557 of 2 November 2007, which is based on the principles of the same regulatory provisions. The proposed general operating rules must be submitted to ASN in the operating authorization application file, which must be processed by the authority within a deadline of one year. General operating rules aim to protect the interests covered in Article L.593-1 of the

Environment Code: nuclear safety, radiation protection, preventing and fighting against malicious acts, public health, and protection of nature and the environment. Provisions to support and favour civil security actions in the event of an accident are covered by on-site emergency plans.

Any subsequent modification of these general operating rules must be submitted to ASN for approval, or, for certain modifications, must be authorized by an internal control body organized by the operator that offers sufficient guarantees of quality, independence and transparency.

20.1.1. Content of general operating rules

In the general operating rules, the first group of chapters deals with the organization of operations (Chapter I), the organization of quality in operations (Chapter II) and the processes for managing operating documents (Chapter VIII). These are the prerequisites for safe operation, which implies that operating documents are prepared in advance and are used by personnel with defined skills and training who work according to a clearly explained allocation of responsibilities.

The second group of chapters deals with the organization of radiation protection (Chapter IV) and radioactive effluent discharge procedures (Chapter V). They are based on general regulatory texts concerning radiation protection and the authorizations for radioactive effluent discharge specific to each site.

They are followed by the operational limits and conditions mentioned previously (Chapter III) that deal with the normal or 'degraded' facility operating mode and define the conditions for maintaining the facility in a safe state, consistent with the safety studies conducted in the design phase.

The periodic inspection and test programmes for systems (Chapter IX) and the physical core testing programmes (Chapter X) are used to periodically check compliance with the requirements presented in the safety demonstration and to detect any deterioration of equipment performance in order to prevent failures.

Finally, the general operating rules define the procedures to be followed in the event of an incident or accident (Chapter VI).

The rest of this chapter will focus on the last three groups.

Only Chapters III, VI, IX, and X of the general operating rules must be formally approved by ASN.

The content of the general operating rules will soon be stipulated in a decision issued by ASN. Further information will likely be added to various aspects (maintenance, preventing and mitigating hazards, operating principles applicable in severe accident situations, limiting nuisances due to reactor operation, on-site transport of hazardous materials, etc.).

20.1.2. Limits of general operating rules

General operating rules do not cover protecting the facility in its capacity as a means of generating electricity. Any rule that is not associated with the nuclear safety demonstration is covered in other documents on operations or organization. This involves, for example, aspects regarding ways to improve the availability or efficiency of the facility.

It is also important to note that control and operating rules for equipment subject to a sufficiently detailed regulatory baseline are not included in the general operating rules. This is the case with control measures for pressure equipment making up the main primary system and the main secondary system, which are covered by regulations concerning what is now known as 'nuclear pressure equipment'.

20.2. Operational limits and conditions

The design and safety studies determine the limits within which the facility should be maintained so that, if an incident or accident occurs, the facility stays within the bounds of the situations studied, which have served as the basis for authorizations granted for facility operation. For operational purposes, these limits are translated into authorized operating modes.

This involves:

- limiting the normal operating modes of the facility so that it stays within limits that ensure the confinement barriers will function correctly during the incidents and accidents included in the design of protection systems and engineered safety systems;
- stipulating the appropriate availability for control, protection, and engineered safety systems in all the authorized domains of the reactor so that the systems necessary to implement incident or accident operating procedures are available, if necessary;
- determining the procedures to be followed in the event of unavailability of an equipment item or system that should normally be available in the operating mode of the facility or if a parameter important to safety deviates.

The operational limits and conditions translate these limits in terms that can be directly used during the various phases of normal reactor operation[634]. By their strict application, the structures, systems, and components important to safety remain in a state that complies with the requirements assigned to them and avoids significant damage to the reactor core should an accident occur.

[634] They therefore do not apply to incident or accident operations where safety is guaranteed by complying with dedicated operating procedures.

20.2.1. Content of operational limits and conditions

The operational limits and conditions consist of three sections:

- Section I is a standard document, applicable to a reactor type (plant series, etc.);
- Section II contains additions to the standard document that are specific to a site or reactor;
- Section III contains amendments to the standard document, applicable to a reactor type.

The standard document consists of nine chapters.

The first chapter, entitled General Information, contains policy information used to develop the operational limits and conditions; it reviews their role, defines the authorized operating modes of the reactor and the rules to be applied if one or several events occur.

The following six chapters deal with requirements for the various operating modes, from the state in which the reactor is generating electricity to the state where the core is completely unloaded.

The eighth chapter, entitled Definitions, defines certain terms used in the standard document of the operational limits and conditions.

The ninth chapter, entitled Grid Disturbance, contains variations on the requirements applicable to the six operating modes, which can only be applied in the specific situation where a widespread incident has occurred on the power grid.

The operational limits and conditions are written so that the requirements to be met in an operating mode are self-explanatory. For each operating mode, the requirements concern:

- controlling reactivity,
- fuel cooling,
- confinement of radioactive substances,
- cross-system and support functions[635].

The operational limits and conditions also introduced the concept of ‘nuclear steam supply system normal operating function’, associated with the accident operating procedure strategy based on the ‘state-oriented approach’ (SOA), by defining a list of functions for which loss of function means that the reactor (nuclear steam supply system) can no longer be maintained as is or in a fallback state by normal operating procedures and that, for at least one operating mode, an SOA means of substitution must be used to bring the reactor back to a safe state.

[635] The cross-system and support functions correspond to equipment and systems that provide the fluids required for the facility to operate correctly (electricity, air, cooling water, etc.).

Several concepts used in the operational limits and conditions deserve a specific explanation.

20.2.1.1. Operating modes and standard states

Six operating modes have been defined for pressurized water reactors:

- reactor at power (generating electricity),
- reactor in normal shutdown state cooled by the steam generators,
- reactor in normal shutdown state cooled by the residual heat removal system,
- maintenance outage,
- outage for refuelling only,
- reactor fully unloaded.

For each operating mode, the operational limits and conditions indicate the equipment and support functions that must be available so that the fundamental safety functions are ensured, as well as the procedures to be followed if an equipment item is unavailable.

The limits of these operating modes are expressed as a combination of conditions relative to reactor power level, core reactivity and the means of controlling it (RCCAs, boron concentration), average pressure and temperature values of the reactor coolant system, and, if applicable, the water level in the reactor coolant system.

The operating modes cover the 'standard states' of a reactor (corresponding to the domains defined in design and operating studies, consisting of the reactor coolant system pressure and temperature limits), while taking into account more specific conditions, such as whether or not the reactor coolant system is open. These standard states are as follows (the numerical values correspond to 1300 MWe reactors and are given for information only):

1. Outage for refuelling only: in this state (cold shutdown), the reactor pool is filled with borated water at 2385 ppm boron, the closure head is removed, the reactor coolant system is at atmospheric pressure, its temperature between 10°C and 60°C, and reactor residual heat is removed by the RHRS.
2. Maintenance outage with the reactor coolant system sufficiently open and the core loaded (cold shutdown): the pressure and temperature conditions are the same as for the previous state, but the reactor pool is not filled with water. In this state, the water level in the reactor coolant system may be lowered to a level close to the midplane of the reactor coolant system piping. This state is used to install or remove blanking plates (or closure plates) at the connection between the reactor coolant loops and the steam generator inlet plenums[636].

[636] See figures 22.1 and 23.2 showing the location of these plates. They are fitted when it is necessary to inspect the steam generator tubes without unloading the fuel.

3. Maintenance outage with the reactor coolant system partially open (cold shutdown): in this state, the reactor coolant system is at the pressure of the containment atmosphere and can be drained to a level close to the midplane of the reactor coolant system piping (to then be depressurized to 200 millibars absolute).
4. Maintenance outage with the reactor coolant system closed at a pressure below 5 bars absolute (cold shutdown).
5. Normal cold shutdown where the reactor is cooled using the RHRS: in this state, the reactor coolant system is closed and filled with water. Its pressure may reach 31 bars absolute and its temperature is at 90°C.
6. Intermediate shutdown with cooling performed by the RHRS using 'single-phase' reactor coolant system water: in this state, the temperature of the reactor coolant system water may reach 180°C and its pressure 31 bars absolute. In the absence of a steam blanket in the pressurizer, pressure is controlled by the chemical and volume control system (CVCS). The reactor coolant system is protected from overpressure by the RHRS valves.
7. Intermediate shutdown achieved using 'two-phase' reactor coolant system water under 'RHRS connected' conditions: this state is different from the previous state due to the presence of steam in the pressurizer, which controls pressure. The reactor can be cooled either by the RHRS or by one or more steam generator(s).
8. Intermediate shutdown achieved using 'two-phase' reactor coolant system water, where residual heat is removed by the steam generators (SGs) and the RHRS is isolated (normal shutdown using SGs), the reactor coolant system temperature remaining compatible with connection of the RHRS.
9. Intermediate shutdown achieved using 'two-phase' reactor coolant system water and the steam generators: this state is characterized by an average RCS water temperature between 160°C and 295°C and by pressure between 27 and 139 bars absolute, with the average pressure-temperature pair remaining below a defined range (see Section 20.2.2).
10. Hot shutdown (at zero power, normal shutdown achieved using steam generators): in this state, the reactor is subcritical. The average pressure and temperature conditions of the reactor coolant system extend from those given for the state defined above to the conditions acceptable for reactor startup.
11. Approach to criticality (belonging to the 'reactor at power' mode); in this state, the boron present in the reactor coolant system water is diluted until the boric acid concentration reaches the level required to attain criticality.
12. Hot standby (reactor at power): this state corresponds to the reactor startup conditions, from criticality to a power level below or equal to 2% of nominal power; the reactor is critical.
13. Reactor at power: power is between 2% and 100% of nominal power.

20.2.1.2. Requirements and unavailability

Each operating mode, or each standard state, is associated with a specification defining the positions of the RCCAs, a list of equipment or systems required for safety, chemical specifications for various fluids and other requirements.

Each chapter of the operational limits and conditions dedicated to one of the six operating modes is composed of two parts: the first part covering requirements for each safety function and the second part consisting of tables indicating the procedures to be followed if it is not possible to comply with one of the requirements in the first part. These deviations are called 'events' and represent partial or total unavailability of a safety function. When an equipment item or system ensuring a safety function required by the operational limits and conditions becomes unavailable or is found to be unavailable, reactor operating conditions are degraded and the procedures to be followed, as defined in the operational limits and conditions, aim to reduce the resulting risks. For this purpose, the operational limits and conditions may require fallback of the reactor to a standard state that is considered safer.

Unavailability may be:

- inadvertent if it results from the unexpected occurrence of an operating malfunction in the concerned equipment, detected by one of the means available to the operator,
- planned according to an operating rule or requirement (for preventive maintenance operations or periodic tests),
- due to other causes, for example if an equipment change or requalification has been performed.

20.2.1.3. Fallback states and time required to reach them

A fallback state is a state that can be reached and in which the facility can be maintained in acceptable safety conditions, given the equipment and/or systems that are unavailable and the initial state of the reactor.

This concept obviously does not apply to unavailability situations that directly cause reactor shutdown. For example, unavailability of the electrical power supply to the RCCA drive mechanisms causes these assemblies to drop by gravity because they are no longer held in place.

Regarding unavailability of equipment important to safety, the operational limits and conditions define a state of fallback among the standard states and a time delay to initiate fallback that takes into account an estimation of the increased risk due to unavailability.

Two aspects are involved in the choice of fallback state:

- there are one or more standard state(s) in which the defective equipment or system is no longer necessary or, at least, is less important to safety;

- it is possible to change from the initial state to the fallback state using normal operating procedures. Fallback must be executed in compliance with the maximum fallback transient time periods, indicated in the General Information chapter of the operational limits and conditions.

Fallback initiation time delays were determined pragmatically, considering two additional conditions:

- the authorized time delay aims to allow minimum maintenance to be performed within a realistic time frame in order to remedy the situation. If, given the risk involved, this time period is not long enough for the required maintenance, it is preferable to proceed with fallback immediately;
- the duration of sustained operation in the presence of unavailability must not be too long, and must be set according to the actual time required for the maintenance operation, to discourage the operator from leaving the reactor in a degraded state.

Probabilistic safety assessments provide insight into the best response, in terms of the actions to be taken and the authorized maximum time for accomplishing these tasks (see Section 14.5.3.2).

An example of fallback times and states is given below, showing how they relate to facility design.

The steam generator emergency feedwater system (EFWS) for 1300 MWe reactors is equipped with two motor-driven pumps and two turbine-driven pumps. With the reactor at power, the unplanned unavailability of any of these pumps is tolerated for three days and the fallback state is the ‘two-phase’ intermediate shutdown in RHRS conditions, with the RHRS connected.

For 900 MWe reactors for which the EFWS has two motor-driven pumps but only one turbine-driven pump, the unavailability of a motor-driven pump is tolerated for three days as in the previous case, whereas unavailability of the turbine-driven pump is only tolerated for 24 h. The fallback state is the same.

20.2.1.4. Events and event groups

Events are classified into two groups, depending on the importance of their consequences for safety.

Group 1 events involve deviations that compromise compliance with the requirements and assumptions of the safety demonstration. It is prohibited to voluntarily cause a Group 1 event, except for those that are clearly identified and authorized in the limit conditions (see below) of the operational limits and conditions and in the test rules in Chapters IX and X. An operator may not change the operating state if doing so would lead to a Group 1 event. Reactor criticality with a Group 1 event underway is prohibited.

The operational task to be performed for a Group 1 event generally requires initiation of reactor fallback within a time period ranging from one hour to seven days.

Group 2 includes deviations that reduce the reliability of a function important to safety, without directly impacting the safety demonstration. In this regard, it is acceptable to voluntarily cause a Group 2 event, for example, to perform a preventive maintenance operation or periodic test, provided the same rules as those for an inadvertent event are applied (compliance with required repair time, application of corrective measures, compliance with rules on event combinations – see the following section).

An event is 'cleared' after repair and satisfactory requalification of the incriminated equipment or system, or when the reactor is in a state where the unavailable safety function is not required.

Section 14.5.3.2 of this book describes the contribution that probabilistic safety assessments have made to defining the rules to be adopted with regard to Group 1 and Group 2 events.

20.2.1.5. Combined types of unavailability

Only individual cases of unavailability were discussed above. It is possible that several instances of unavailability occur simultaneously. The operational limits and conditions also indicate the procedures to follow in such cases.

In addition, rules have been established with regard to combined events of the same group (there is no concept for combined events belonging to different groups). For Group 1, a combination of events reduces the fallback initiation time. In the case of a combination of more than two Group 1 events affecting different plant systems, reactor fallback must be initiated within an hour. The reactor must be brought to the fallback state corresponding to one of the events, that which is closest to the maintenance outage operating mode. For Group 2, reactor fallback, or a shorter repair time, are required starting from a certain number of events.

For example, while the sole failure of a steam generator emergency feedwater supply pump on a 1300 MWe reactor is tolerated for three days, with the reactor at power, this failure may not be combined for more than 24 h with the failure of a medium- or low-head safety injection pump.

20.2.1.6. Concepts of 'boundary condition' and 'specific requirement'

Specific requirements and boundary conditions were introduced in the operational limits and conditions for certain situations, in addition to general requirements.

A boundary condition allows operation of the reactor when it is not in strict compliance with a general requirement. This boundary condition must only be used for the amount of time strictly necessary to fulfil operating imperatives (operation, maintenance, tests). Boundary conditions may be associated with temporary corrective measures[637] that must be complied with. Resorting to a boundary condition is considered as a Group 1 event.

[637] In French: *palliative*. These measures are referred to as 'temporary' because they allow the plant to return to an operational state, but do not address the root cause of the failure.

A specific requirement also allows the reactor to operate when it is not in strict compliance with a general requirement, but this case involves a variant for which the safety demonstration is ensured. A specific requirement may be associated with implementation conditions that must be complied with.

20.2.2. Average pressure and temperature range of the reactor coolant system

Figure 20.1 illustrates the limits of the average pressure and temperature range of the reactor coolant system in the various states of the reactor (these limits define what is referred to as the 'operating domain'). The indications show how design choices are transposed into the limits of an authorized operating domain.

Maintaining the RCS average pressure-temperature pair in the defined domain guarantees compliance with the safety limits associated with the second confinement barrier, the reactor coolant system.

In particular:

- compliance with the limit [Psat, (Tsat - 30°C)] – see the saturation curves in Figure 20.1 – leaves a sufficient operating range for the pressurizer and avoids boiling in the rest of the reactor coolant system;
- compliance with the limit [Psat, (Tsat - 110°C)] minimizes the maximum temperature difference between the pressurizer and the hot leg of the reactor coolant system, thereby limiting fatigue on the pressurizer and the surge line (which links the pressurizer to one of the hot legs), caused by the frequent water movements that occur in this line when switching between cold shutdown and hot shutdown and during power transients;
- compliance with the limit [(Psat + 110 bars), Tsat] makes it possible to keep the pressure difference between the reactor coolant system and the secondary system from exceeding 110 bars, the maximum value used for designing the steam generators;
- compliance with the lower temperature limit (160°C) of the two-phase intermediate shutdown state with the steam generators makes it possible to maintain a margin relative to the NDTT[638] of the reactor vessel metal at end of life for a pressure of 172.3 bars (pressurizer valve opening threshold). Below this temperature, the reactor coolant system must be cooled and protected against overpressure by the residual heat removal system (RHRS);
- the lower temperature limit (120°C) of the two-phase intermediate state with RHRS connected is a value below which the pressurizer 'steam blanket' must

[638] Nil Ductility Transition Temperature: temperature below which the metal exhibits fragile behaviour and may suddenly break in the presence of a defect and in response to sudden pressurization. This temperature, originally less than 0°C, increases under irradiation by neutrons due to an accumulation of 'damage' in the crystal lattice.

not be maintained. This limit is defined in the design basis for the pressurizer surge line.

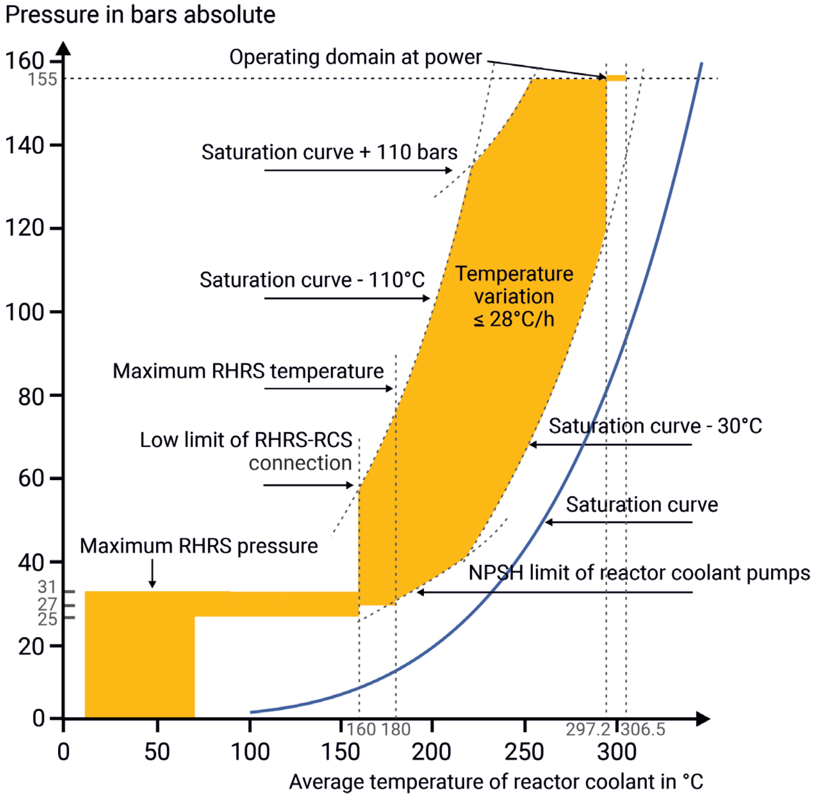


Figure 20.1. Average pressure and temperature domains (1300 MWe). IRSN.

Other pressure or temperature values are based on technological limits which are briefly substantiated as follows:

- the RHR system must not be connected to the reactor coolant system above 31 bars absolute to keep a sufficient margin relative to the set pressure threshold for the safety valves in this system;
- the reactor coolant pumps cannot be maintained in service below 25 bars (this value is 27 bars for reactor coolant system water temperatures above 160°C);
- satisfactory operation of the RCCA drive mechanisms is not guaranteed below 4.5 bars absolute;
- crystallization of boric acid is avoided with a sufficient margin if the water temperature is above 10°C for a solution with 2385 ppm boron;

- operation of at least one of the reactor coolant pumps is no longer necessary above 70°C;
- 90°C is the maximum temperature for ensuring reactor coolant system venting without the risk of vaporization after a shutdown for reloading or maintenance.

20.2.3. Changes in operational limits and conditions

At the beginning of the nuclear power plant programme, French pressurized water nuclear reactors were operated with operational limits and conditions adapted from those provided by the licensor, Westinghouse. They only involved operation at power, and only the protection systems and engineered safety systems were covered.

The operational tasks to be performed in the event of equipment unavailability and the definition of fallback states were studied after the Three Mile Island accident.

Operating experience in France and in other countries then showed that safety in shutdown situations required systematic study of the requirements in terms of available equipment in these situations. These studies led to the adoption, in 1986, of operational limits and conditions for states in which the reactor coolant fluid is below 90°C. This approach involved defining a minimum list of equipment whose availability is necessary to guarantee reactor safety while allowing equipment maintenance.

Studies on the actions to take in incident and accident situations also led to extending the scope covered by the operational limits and conditions to include measurement systems necessary for diagnosing these situations and for choosing the appropriate operating procedures.

Specifications were also defined for related systems such as ventilation systems, fire protection systems and radioactivity monitoring systems. It is important that systems contributing to facility safety, even less directly, should not remain unavailable for an unlimited time.

Operating experience and probabilistic safety assessments later led to taking multiple failures into account as well (see Chapter 13 on the ‘complementary domain’), considering that they may occur not only when the reactor is generating, but also in other reactor states. Operational limits and conditions were then defined for equipment considered necessary for managing these situations.

The ‘baseline’ for core-melt accidents, situations taken into account for the EPR design, was transposed into the operational limits and conditions for the Flamanville 3 EPR. As periodic reviews were conducted, the operational limits and conditions of 900 MWe, 1300 MWe, and 1450 MWe reactors incorporated this baseline. The first reactors for which this was done were the 1300 MWe reactors (when their third ten-yearly outage took place), then the 900 MWe reactors as part of their fourth ten-yearly outage.

The fourth ten-yearly outage of 900 MWe reactors was also an opportunity to start including hazards in their operational limits and conditions, which was also done for the Flamanville 3 EPR. The third ten-yearly outage of 1300 MWe reactors and the second ten-yearly outage of 1450 MWe reactors provided the opportunity to partially introduce information concerning hazards in the operational limits and conditions.

When situations occur where it does not seem possible to comply with the operational limits and conditions or where they could lead to a state considered unfavourable for safety, Électricité de France (EDF) modifies the operational limits and conditions and submits a declaration to ASN. These modifications are an opportunity to detect ambiguous or inapplicable wording, which must be corrected, but also cases where the operating mode or the facility must be modified to comply with a principle established by the operational limits and conditions that it does not seem advisable to modify.

To give operating personnel a good understanding of operational limits and conditions, it is, however, recommended that these specifications remain sufficiently stable. As part of or following periodic reviews, and as part of operating experience feedback from reactor operation, taking into account changes made to safety 'baselines' may lead to regular or occasional amendments to standard documents for various plant series, but these changes do not affect document usability nor the approach to transposing the safety demonstration into the operational limits and conditions.

20.3. Initial and periodic tests

Startup tests for a nuclear reactor (see Chapter 19) represent a very important phase of preparation for its future operation. In addition to validating design choices, these tests help in developing general operating rules and in training personnel.

Periodic tests of equipment important to safety help to monitor the availability of this equipment and prevent failures.

Periodic test rules for 'items important to protection in the area of nuclear safety' (or 'items important to safety') make up Chapter IX of the general operating rules. The only items important to safety that are not included in the periodic test programmes are those subject to specific, sufficient inspection regulations and those used with certainty for a sufficiently long period during normal operation (in conditions comparable to incident or accident situations) and monitored by instruments that guarantee rapid detection of deviations.

Chapter IX of the general operating rules includes a section that defines the general objective of periodic tests, their scope, the principles to ensure their representativeness, the principles for including measurement uncertainty, and the conditions of satisfactory test completion and of handling detected deviations.

Periodic tests help provide assurance regarding the following points:

- the absence of unfavourable changes in the characteristics of the relevant equipment or system compared to those used for their design,
- compliance with the assumptions used for accident studies (the values used are often different than nominal operating values),
- availability of equipment and systems for preventing, controlling, or mitigating an accident.

Each function important to nuclear safety is analysed to exhaustively determine all inspections that must be conducted to satisfactorily guarantee the availability of equipment whose functional capability is necessary. This analysis must ensure consistency between the initial compliance tests performed during reactor construction and startup, or during later changes in the facility, and the periodic tests planned to maintain these characteristics over time.

For an elementary plant system, this analysis becomes a periodic testing rule that stipulates the performance conditions on which test representativeness depends, the criteria to be met (qualitative or quantitative), and the time interval between two identical tests.

If the operator cannot conduct certain periodic tests in conditions compatible with the operational limits and conditions, applying Chapter IX of the general operating rules, subject to the approval of ASN, serves as a general modification of the operational limits and conditions during these tests.

Test procedures, documents directly used by those in charge of performing periodic tests, are written by facility personnel using the test rules, taking into account the specific features of each facility. Each worker has their own document in which they note the results and which serves as a test report.

The periodic testing rules must be revised regularly based on facility modifications and operating experience feedback. Feedback from construction, commissioning and operation is a source of information to be used whenever necessary or appropriate. This feedback may show that:

- failure frequency observed by inspections and tests is greater than expected, or that breakdowns occur during transients. The frequency of periodic tests can then be adjusted accordingly;
- tests are not performed in sufficiently representative conditions. Test conditions are then modified, as in the case of the tests at the steam generator emergency feedwater turbine-driven pumps for 900 MWe reactors;
- the difficulty of certain manual tests is the cause of incidents, as was the case for certain tests of the 900 MWe reactor protection system. A programmable logic controller was designed, tested, and implemented in these reactors;
- tests performed too frequently or under conditions that are too severe are the cause of equipment damage and premature ageing. The programmes are then modified accordingly. The most characteristic example concerns the diesel

generators that ‘fatigued’ due to unnecessary rapid startups. Specific test conditions were defined that require only a ‘soft’ startup of the diesel generators, where the corresponding order is cancelled automatically in case of real triggering. This automatic cancellation is also covered by tests;

- endurance tests conducted in the factory by the manufacturer are not representative of on-site operating conditions and do not cover the influence of the rest of the system;
- measurement uncertainty is not taken into account satisfactorily in the periodic tests. Testing rules have been changed to systematically consider uncertainty in measurements obtained using field sensors. For measurements obtained using specific test instrumentation, EDF has written guides on how to consider uncertainty.

In general, whenever the conditions of a periodic test require modifying the state of an equipment item or a system, specific precautions are applicable. The temporary measures and devices used to conduct the test and liable to disturb or prevent the proper operation of protection systems and engineered safety systems operating exclusively on demand should be checked to ensure that they have all been removed.

20.4. Incident and accident operating procedures

The principles of the procedures to be followed if an incident or accident occurs are described in Chapter VI of the general operating rules.

The operating strategies and practices to be used (Figure 20.2) in an incident or accident situation (referred to generally as ‘procedures’) are discussed in various documents made available to the operating crews. This organization was one of the lessons learned from the Three Mile Island accident.

The first document, called an Operating Rule, is a strategic, supporting, and educational document, used during training periods.

The second, which constitutes the Reference Operating Procedure, is a document that serves as an intermediary between the operating rule and the third document, which is the Unit Operating Procedure, the only document used in real time in the event of an incident or accident. The reference operating procedure is written based on the operating rule and details the actions for implementing the strategy adopted. The operating procedure for each unit incorporates its specific features (identification of equipment, change status, specific dimensions, etc.). An internal directive specific to the operator sets the limits of acceptable differences between the reference operating procedures and the unit operating procedures. In particular, the operating strategy may not be modified locally.

The reference operating procedures have been subject to many tests on simulators to improve their presentation and reduce the risk of errors.

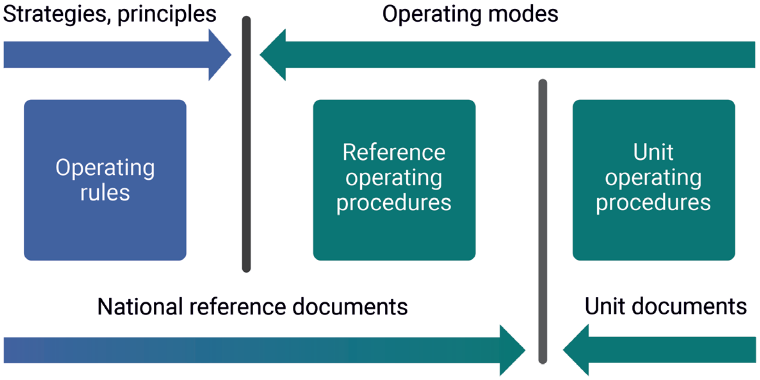

Strategies, principles
Operating modes
Operating rules
Reference operating procedures
Unit operating procedures
National reference documents
Unit documents

Figure 20.2. Organization of incident and accident operating documents. IRSN.

In French reactors (up to and including the N4 series), each operator has a document specific to their function in the control room (core and reactor coolant system operation, secondary system operation). The Supervisor (see Section 25.3.1) also has a specific document for overseeing the operators' actions and ensuring their coordination.

When an incident or accident operating procedure is applied, the Shift Manager, and then the Safety Engineer, constantly monitor the state of the reactor according to a specific procedure. They thus ensure diversification for diagnostics and monitor the effectiveness of the measures taken.

EPR design studies led EDF to explore changes to the operating crew. For Flamanville 3, it had planned for:

- operation in incident or accident situations that is identical to that described above,
- for normal operation, only one operator (the 'action' operator) in charge of the core, the reactor coolant system, and the secondary system, with the other operator monitoring the state of the facility and activities in the control room (the 'strategy' operator).

However, the validation campaigns conducted by EDF on a full-scale simulator in the early 2010s led to abandoning this choice and reusing provisions adopted for previous reactors (see Section 25.3).

In the operating procedures, since the automatic operating conditions of the system for protecting and starting engineered safety systems are those of the incident and accident studies of the safety analysis report, the short-term actions that operators are asked to perform must also comply with these studies.

Following the Three Mile Island accident, all the procedures were revised by EDF in order to:

- take into account accident management over a much longer time period,

- base procedures on realistic physical studies (the studies for the safety analysis report are based on conservative assumptions),
- identify the operating strategy best suited to the medium and long term,
- ensure that the documents were usable.

To develop an operating procedure, multiple aspects must be carefully examined: the subject matter covered by the procedure, the symptoms and information for choosing the most suitable operating strategies, the interfaces with operating documents for the unaffected parts of the facility, the exhaustive list of equipment items, including information equipment items, that are necessary to apply the procedure, and their qualification including their measurement range and their accuracy.

As part of this review, the operator must consider different parts of the general operating rules. An equipment item necessary for applying a procedure must be among the available equipment items in the initial state of the unit corresponding to the accident (in compliance with operational limits and conditions) and must have the expected characteristics, accuracy and reliability (periodic tests).

Two examples, already dating back several years, can be given here of how procedures have changed.

The first concerns the event operating strategy in the event of steam generator tube rupture. Initially, the drop in pressure in the reactor coolant system was obtained by cooling the reactor coolant fluid using steam generators in good condition, associated with intentional opening of the pressurizer relief system. Since the spring-loaded valves used in this system had a non-negligible risk of jamming in open position, this intentional opening was eliminated. The drop in pressure was then only the result of reactor coolant fluid cooling. The later replacement of the spring-loaded valves by SEBIM^{TM} tandem valves, which do not involve the same risk of jamming open, did not, however, lead to abandoning this operating strategy which was satisfactory.

The second example concerns accident operation and the consequences of poor accuracy of the analogue water level measurement device in the reactor vessel when this level is very low (uncertainty around 30% instead of the expected 12%). The conditions for reactor coolant pump shutdown in these conditions had to be changed.

Chapter 21
Operating Experience Feedback from Events: Rules and Practices

21.1. Background

In 1963, an internal report by the manager of atomic piles at the French Atomic Energy Commission (CEA) noted that "the most severe accidents often result from coinciding incidents that, occurring individually, may not have been serious". It also mentioned that "progress in the art of nuclear safety unfortunately comes in great part from the analysis of accidents that have in fact taken place". Then in the 1970s, with the deployment of the nuclear power plant fleet in France, the first incident files were prepared, mainly to provide data for equipment reliability studies. Because the nuclear facilities had not yet existed for very long, and due to industrial development problems, operators mainly focused on the real consequences of the incidents. If there were no consequences, the incidents were not considered important. In different contexts around the world, accidents involving the nuclear industry gradually brought to light other major principles, revealing the usefulness of operating experience feedback. Long-term, shared corrective actions and international sharing and transparency of experience emerged as fundamental.

In 1973, during a presentation to the IAEA of the general principles and practical applications of power reactor safety analyses in France, Jean Bourgeois[639] stated: "In conclusion, one point should be emphasized [...], that is, how important it is in terms of safety to gather experience from the operation of reactors in service... We may not

[639] The director of IPSN from 1976 to 1978.

currently be getting the fullest possible benefit from the lessons learned from incidents and accidents in reactors around the world… Gathering information and interpreting accidents are indeed difficult tasks. But […] we should make the effort to have a more complete exchange."

In 1979, the accident at Three Mile Island (TMI) occurred in the USA. The report issued by the Kemeny commission of inquiry noted that several earlier incidents could have been considered as precursors, but they were not analysed and taken into account (see Chapter 32). The principle by which 'no real consequences amounts to no importance' was thus brought into question. The TMI accident caused renewed interest in 'operating experience feedback' (OPEX) at the international level and resulted in according greater importance to warning signs and precursors.

From that point forward, it was recognized that an accident is due to a sequence of multiple failures, involving both equipment failures and human errors, and that it was highly probable that some of these failures occurred in minor incidents which could initiate much more serious accident scenarios.

In 1986, the Chernobyl accident occurred in Ukraine. Beyond design shortcomings, this major accident made it obvious that operating practices were critical in maintaining a high level of safety in nuclear facilities. Whereas post-TMI actions focused on the control room, operating systems, and the study of accident situations, especially those that may result from multiple failures, the Chernobyl accident raised questions about the human element, organizations and 'normal' operation. The internationalization of operating experience feedback reached a new level. In 1991, the OECD and IAEA created the International Nuclear Events Scale (INES), based on a severity scale created in France after the Chernobyl accident (see Section 34.10). Initially designed to classify events occurring in nuclear power plants, this scale, mainly for public relations purposes, was extended and adapted so that it could be applied to all facilities related to the civil nuclear industry.

In 2011, the Fukushima Daiichi nuclear power plant accident occurred in Japan. Although 40 years of operating experience feedback – as well as studies and R&D – had significantly contributed to improving the safety level of facilities and their operation, it became clear that certain questions had not been considered in all countries.

Numerous technological and scientific changes had been made over the span of 40 years, in parallel with profound industrial, social, economic, cultural and political changes. The purpose of operating experience feedback is to learn lessons from adverse events that have marked and continue to mark the operation of nuclear reactors, with the goal of maintaining and improving performance in the area of risk control. Although the major accidents have mainly involved power reactors (Three Mile Island, Chernobyl, and Fukushima Daiichi), OPEX approaches of course apply to all facilities using radioactive materials or sources of radiation, whether for civil, military, industrial, research[640], or health and medical purposes.

[640] The IRSN book entitled Elements of Nuclear Safety – Research Reactors, J. Couturier et al., Science and Technology Series, IRSN/EDP Sciences, 2019, offers illustrations of OPEX from events that occurred in research reactors.

In 40 years, the subject of operating experience feedback has considerably evolved from design OPEX to operating OPEX, based on representations of the analysed 'system' that have evolved themselves (from a purely technical system to a sociotechnical system[641]), influenced by events and regulations.

Situating the historical and contextual background helps to understand the problems encountered when attempting to reap the full benefits of operating experience feedback in operational risk management systems. However, it is fundamental to manage operating experience feedback so that it is a true source of learning, capable of driving effective change in technical systems, practices and work organization.

21.2. Objectives of an operating experience feedback system

An operating experience feedback system has several objectives:

- analyse the events encountered, share lessons with and between stakeholders, implement appropriate actions and corrective measures to prevent similar events from happening,
- aim to prevent events having causes directly or indirectly linked with past events,
- anticipate any generic problems that could affect the operation of a significant portion of the reactors in the nuclear power plant fleet,
- confirm design validity or identify possibilities for improvement,
- improve performance in all areas through changes in equipment, operating methods, organizations and by taking into account all components (nuclear safety, radiation protection, environment, availability, etc.) through collective analysis of the events.

Operationally, an OPEX system aims to produce knowledge and determine actions from this knowledge. The primary function of an OPEX system is thus to analyse and understand. It must be possible to share this understanding with stakeholders and take lasting action on any problems in the sociotechnical system.

▶ Analyse and understand

Learning lessons from an event (or set of events) first makes it possible to acquire new knowledge or consolidate existing knowledge. Knowledge from an event varies according to what is taken into account, whether this be the event detection conditions, the event sequence, human, organizational and technical causes involved in

[641] System composed of technical (physical) elements and human elements, formally organized according to standards, rules and roles, in order to attain predefined objectives.

producing the detected deviation, the consequences this deviation had or could have had, and systems ('lines of defence') that 'worked' and those that did not 'work'.

Lessons learned from events can help build on technical knowledge, improve the knowledge of real operating practices, refine the understanding of a particular question (by monitoring indicators), or identify a specific new question that emerges from the recurrence of a type of event or, inversely, that is highlighted by a surprising event.

▶ Sharing experience

Operating experience feedback offers mainly a collective advantage. To be useful, the knowledge from operating experience feedback must be shareable between those who produce it and those who could benefit from it. For an operator, what matters is delivering the right information from operating experience feedback to the right people at the right time.

Sharing experience requires setting up systems to store, disseminate, and find information, not only raw information but information that has been processed to make it usable.

▶ Taking action

An operating experience feedback system defines actions and measures that avoid the recurrence of a given event, an event of the same type, or the occurrence of event scenarios belonging to the same family. These actions and measures may concern:

- equipment reliability,
- reliability of organizations,
- professionalism of actors.

It is possible to act on organizations, work practices or the technical system. Since these aspects (or 'dimensions') interact, an effective modification will most often affect all of them. The lessons learned from experience may also present an opportunity to upgrade risk control requirements.

It is important to note that corrective action regarding an event may require that rapid temporary (corrective) measures be taken pending definitive measures.

21.3. Components of an operating experience feedback system – Regulations

An operating experience feedback system may be described as a system composed of inputs, processing actions and outputs. The objectives assigned to this system determine the types of events to be processed (the inputs), a set of means (methods, tools, organization, management) for processing events, any new technical or organizational measures for the facilities and, more generally, individual and collective learning (outputs).

An operating experience feedback system therefore includes:

- methods: they concern the analysis of specific events, the analysis of trends or the thematic analysis of a set of events. The methods used serve to guide analysts, so they can identify the facts and actions actually carried out during the events (it is not enough to describe those that were expected). They offer the conditions for making information available, which in turn facilitates sharing the understanding derived from these analyses;
- tools: specifically, this entails 'structuring' event databases for the purpose of extracting information (through sorting, queries, etc.) and disseminating knowledge. Designing tools for efficiently storing and providing information about events is a complex exercise. Structuring[642] information appropriately is important; otherwise, in time, the results provided may be irrelevant or unusable. Beyond the initial query results extracted from the structured event data, which provides a first-level analysis of these events, the expertise of a data analyst is necessary to derive any relevant knowledge;
- an organization: for everyone concerned, this defines the roles and responsibilities in design, management and use of the operating experience feedback system, the decision-making processes, the communication processes, the conditions of sharing, etc.;
- management systems: necessary to execute and coordinate the processes involved and ensure information is shared and circulated. Like any learning and decision-making process, an operating experience feedback system requires management capabilities and attitudes that promote information reporting, in compliance with safety culture. Making relevant data available is fundamental and essential to ensuring that an operating experience feedback system functions well.

Beyond the means allocated to implementing an operating experience feedback system and the operational and strategic choices made when it is set up, the regulatory component (see the Focus feature below) introduces important requirements for the system's inputs, its operation and its outputs. Supervisory administrative authorities are involved in decision-making and control of the operating experience feedback system. They are stakeholders in the global learning loop.

Beyond the specific equipment of the facilities in question, the lessons learned from experience are often cross-functional, which may lead to broadening the scope of these lessons to other facilities, other organizations, or even other industrial sectors. It can be beneficial to exchange views between fields that at first glance seem to have few or no points in common.

[642] In terms of typology (nuclear safety, radiation protection, environment, availability, etc.), causes (related to equipment, human and organizational factors, etc.), real or potential consequences, disciplines concerned (control, testing, maintenance, etc.).

In 1980, following the accident at Three Mile Island, as indicated in Chapter 3, the Nuclear Energy Agency (NEA) set up the Incident Reporting System (IRS) internationally. This system was designed to collect and disseminate information on incidents in the nuclear power reactors of its member countries, information liable to be relevant across these countries. The member countries of the OECD/NEA represent the major part of the world's nuclear power capacity, equivalent to several hundreds of facilities. Starting in 1995, the IAEA began managing the system, which was open to all countries that had signed the Convention on Nuclear Safety. Later, in 2009, to reflect the growing use of the system, the IRS became the International Reporting System for Operating Experience. National coordinators annually submit those incidents considered the most relevant for experience sharing. In France, IRSN is the national coordinator. In collaboration with Électricité de France (EDF), it regularly selects events that have occurred in the French nuclear power plant fleet that may be relevant for IRS. It then submits the corresponding sheets to the IAEA. Periodic meetings organized by the IAEA highlight the lessons that each country has learned from its difficulties. This ensures that experience is shared at the international level.

In addition, NEA can set up working groups bringing together specialists from member countries to carry out studies on problems of general interest, based on a series of incident reports associated with the IRS database, involving technical as well as human and organizational aspects. Several studies have been carried out in this manner, for example on incidents occurring during unit outages for refuelling. Following the Fukushima Daiichi nuclear power plant accident, NEA reviewed certain incidents or accidents that were 'precursors' to core-melt accidents (this concept is discussed below, in Section 21.4).

The association WANO (World Association of Nuclear Operators) was created after the Chernobyl accident. It is presented in Section 3.1.5 of this book. Through its Internet site, WANO members can access information on events that have occurred in other facilities. By sharing information, the member-operators can learn from each other's errors and make sure they are not repeated elsewhere.

#FOCUS

Operating experience feedback in official French texts[643]

Decree of 11 December 1963 on nuclear facilities – Article 5-III: "Without prejudice to the application of measures provided for by the regulations in force, any accident or incident, whether or not nuclear in nature, that has or carries the risk of having significant consequences for the nuclear safety of the facilities mentioned in this decree, shall be immediately reported by the operator […]"

[643] These texts are cited according to when they were issued. Some of them have been repealed and reused in various forms in other texts.

Order of 10 August 1984 on the quality of design, construction, and operation of basic nuclear installations – Article 13: "The operator shall report […] significant anomalies or incidents as rapidly as possible. […] The report shall describe the measures already taken or under consideration to limit the extension of the anomaly or incident and, as necessary, to mitigate the consequences. […] Significant anomalies or incidents shall undergo in-depth analysis to accurately determine their causes and their direct or potential consequences on nuclear safety, to derive useful lessons for the activity concerned by the impacted quality and, as necessary, for other activities concerned by quality. […]"

Guide issued on 21 October 2005 by the French Nuclear Safety Authority (ASN), "on the conditions of reporting and enactment of criteria for significant events involving nuclear safety, radiation protection or the environment, applicable to basic nuclear installations and domestic transport of radioactive materials". This guide provides the criteria for reporting significant safety events in pressurized water reactors in its Appendix 6, and the criteria for reporting significant radiation protection events in its Appendix 7, applicable to all basic nuclear installations.

Act No. 2006-686 of 13 June 2006 on Nuclear Transparency and Security – Article 54: "In the event of an incident or accident, whether or not nuclear in nature, that has or carries the risk of having considerable consequences on the safety of the facility or transport conditions, or adversely affecting people, property or the environment by significant exposure to ionizing radiation, the operator of a basic nuclear installation or the person responsible for the transport of radioactive materials shall immediately make the relevant report to ASN and to the State representative in the *département* in which the incident or accident occurred and, if necessary, to the maritime prefect."

In addition, all operators of basic nuclear installations must prepare a report once a year that describes:

- "the nuclear safety and radiation protection measures taken;
- the nuclear safety and radiation protection incidents and accidents that must be reported […] when they occur on the premises of the facility, as well as the preventive and mitigation measures taken to limit their impact on human health and the environment;
- [...]"

This report is made public and copies are sent to the Local Information Commission and the High Committee for Transparency and Information on Nuclear Security (HCTISN).

Decree No. 2007-1557 of 2 November 2007 on basic nuclear installations and controlling nuclear safety in the transport of radioactive materials – Article 11: "[…] the risk control study includes: […]; b) An analysis of the operating experience feedback from similar facilities; […]; d) An analysis of the consequences of potential accidents impacting people and the environment; e) A description of the planned measures for controlling risks, including accident prevention and mitigation of their consequences; […]"

Order of 7 February 2012 setting general rules for basic nuclear installations – Article 2.6.4: "The operator shall report each significant event to ASN as soon as possible. The initial report shall include the characterization of the significant event, the description of the event and its timeline, its real and potential consequences […], and the measures already taken or planned to deal with the event temporarily or definitively" – Article 2.6.5: "The operator shall perform an in-depth analysis of each significant event. […] The operator shall ensure that the preventive, corrective and curative actions decided upon are implemented."

21.4. Operating experience feedback practices adopted for the French nuclear power plant fleet

As indicated above, EDF set up an operating experience feedback system at a very early stage. It was initially aimed at improving equipment reliability. Regarding IRSN, since 1973 it has added to and used a file of events that have occurred in the reactors of the nuclear power plant fleet, based on information provided by EDF.

This has resulted in a considerable amount of coherent and structured information. In particular, it is possible to perform comprehensive searches, for example to identify recurrent or generic events between facilities. The size of the nuclear power plant fleet and the similarity of the reactors make it necessary, however, to rapidly identify a problem that could affect an entire family of facilities and cause the shutdown of a significant part of the electricity generation facilities.

Because of the complexity of nuclear power plants, events occur frequently. This often involves equipment failures that can be resolved without significantly disturbing electricity generation. Much more spectacular events can occur, affecting the turbine generator for electricity generation or the steam systems, potentially immobilizing the reactor in a shutdown state for several months, without disturbing the confinement of radioactive substances. The impact of the second type of event is much more significant than that of the first. However, the first category generally includes the most significant events in terms of nuclear safety and radiation protection. If periodic testing reveals any unavailability in engineered safety features, which are kept on 'standby' during normal unit operation, this is, in theory, more significant for nuclear safety than turbine unavailability.

French practice currently distinguishes between two types of events of differing severity. They are also handled in different ways.

Thus, the definitions in the ASN Guide of 21 October 2005 make a distinction between:

- ‘**relevant events**’ (i.e. those relevant for nuclear safety, radiation protection or the environment) are events whose “immediate importance does not justify an individual analysis, but they may be relevant to the extent that their repetitive character may be indicative of a problem calling for detailed analysis”;
- ‘**significant events’** are events considered as meeting one of the reporting criteria (see the Focus feature below).

Based on the principle that the operational limits and conditions (OLCs) in French nuclear power plants include all requirements concerning the availability of equipment important to reactor safety, as well as the limit values for the various operating parameters, any failure in one of these equipment items leading it to be reported as unavailable or any exceeded threshold is considered as a ‘relevant event’. This definition is relatively clear for the operator.

Since relevant events are not serious in themselves, the operator has no specific notification requirements. However, it must rapidly input these events in a national computer file, managed by EDF, that is accessible to nuclear safety organizations. This event file, part of the SAPHIR tool, can be searched by system, equipment item, plant unit, event date, or date of input to the file.

This file contains not only ‘relevant events’ but all the events that EDF wishes to manage using this computer tool. Each record on a particular event has an index indicating whether it is relevant to nuclear safety, radiation protection or the environment and, as a result, whether it is accessible to nuclear safety organizations.

In general, events relevant to nuclear safety do not call for a detailed analysis and are not ‘precursors’ of severe accidents. These precursors are found in the ‘significant event’ category, which mostly groups together events relevant to nuclear safety that also meet specific criteria initially defined by the Central Service for the Safety of Nuclear Installations after discussions with operators. These criteria had to be accurate enough so that their application could be nearly automatic, without too much variability in interpretation from one facility to another. They were formally defined in 1982. EDF periodically revises the corresponding internal notes to improve the uniformity of application between facilities. In addition, there have been significant changes in how the French safety authority formulates criteria.

The criteria in force for initially reporting significant events in pressurized water reactors are found in Appendices 6, 7, and 8 of the ASN Guide of 21 October 2005. They are reviewed in the Focus feature below. Within EDF, these criteria are restated in a specific directive, DI 100.

A significant event (whether a significant safety event, a significant radiation protection event or a significant environmental event) must be reported to ASN on the same day or the following working day. Within two months, a detailed analysis report must be written following a standard outline. An initial analysis is conducted by the facility in question. If necessary, other specialized departments of EDF contribute to this analysis.

#FOCUS

Significant-event reporting criteria (ASN Guide of 21 October 2005)

Significant events relevant to safety:

1. Reactor trip: manual or automatic activation of automatic reactor shutdown, whether spurious or not, and whatever the state of the reactor, except for intentional activations for scheduled actions (including automatic reactor shutdowns caused by turbine generator trip due to the activation of its protective systems).
2. Activation of an engineered safety system: manual or automatic activation of one of the engineered safety systems, whether spurious or not, except for intentional activations resulting from scheduled actions.
3. Noncompliance with OLCs, or an event that could have led to noncompliance with OLCs if the same event had occurred with the facility in a different state:
   - any noncompliance with one or more permanent conditions defined in the OLCs,
   - any noncompliance with the conditions of an OLC exemption,
   - any exceeded time delays[644] when a fallback mode is not stipulated,
   - any unavailability outside the conditions specified by the general operating rules, not identified beforehand, or identified but not handled according to OLCs.
4. Internal or external hazard: a natural external phenomenon related to human activity, or an internal flood, fire, or another phenomenon liable to affect availability of equipment important to safety.
5. Malicious attempt or act potentially affecting facility safety.
6. Transition to fallback mode in accordance with OLCs or emergency operating procedures in response to unexpected facility behaviour.
7. Event causing or potentially causing multiple failures: unavailability of equipment due to a single failure, affecting all trains of a redundant system, or the same type of equipment in several safety systems.
8. Event or anomaly specific to the main primary system, the main secondary system or pressure equipment in systems connected to them, resulting or

[644] For example, the time required to repair an equipment item.

potentially resulting in an operating condition that was not considered during design or is not covered by existing operating procedures.

9. Design, manufacturing, installation or operating anomaly concerning functional systems and equipment not covered by Criterion 8, resulting or potentially resulting in an operating condition that was not considered and is not covered by design-basis conditions and existing operating procedures.
10. Any other event liable to affect the safety of the facility and considered significant by the operator or the French safety authority.

Significant events relevant to radiation protection:

1. Cases where a regulatory annual individual dose limit has been exceeded, or an unexpected situation possibly leading to such a situation under representative and likely conditions, regardless of exposure type.
2. Unexpected situation leading to a case where the regulatory annual individual dose has been exceeded by one-fourth of the dose limit, during a single instance of exposure, regardless of exposure type.
3. Any significant deviation concerning radiation cleanliness.
4. Any activity (operation, work, modification, inspection, etc.) comprising an important radiation risk, conducted without a formalized radiation protection analysis (substantiation, optimization, limitation) or without exhaustive consideration of the analysis results.
5. Malicious attempt or act that may affect the protection of workers or the public against ionizing radiation.
6. Abnormal situation affecting a sealed source, the activity of which exceeds the exemption thresholds.
7. Deficient sign-posting or non-compliance with technical conditions for access to or presence in specially regulated or prohibited areas (orange and red areas).
8. Non-compensated failure of radiation monitoring systems ensuring the protection of personnel engaged in activities comprising a significant radiation risk.
9. Exceeding the inspection interval for a radiological monitoring device:
   - by more than one month if a permanent collective monitoring device is involved (regulatory interval of one month),
   - by more than three months if other devices are involved (when the verification interval provided for in the general operating rules or the radiation protection reference documentation is between 12 and 60 months).
10. Any other event liable to affect radiation protection that is considered as significant by the operator or the French safety authority.

In the ASN Guide of 21 October 2005, nine criteria are also specified for significant events involving the environment.

Direct exchange between analysts from nuclear safety organizations and the operator may be organized as soon as the initial report has been received. In particular, this is the case when it is assumed that the faults in question could affect part or all of the nuclear power plant fleet or that they could represent a 'precursor' of a severe accident. A rapid response inspection may be performed by ASN.

In general, the definition of safety-relevant events and significant events, closely tied to the thresholds and limits in the operational limits and conditions, allows the operator and the nuclear safety organizations to agree on what is to be initially reported.

For the French nuclear power plant fleet, the average number of significant events has been fairly constant over time, about 10 per reactor per year. Unit outages are the operating periods the most affected, which confirms that these periods are typically characterized by numerous difficulties.

▶ Significant-event analysis methods

When operation began on the first units of the French nuclear power plant fleet, there was no formalized method for reporting operating experience feedback. The collective work of teams at EDF as well as within nuclear safety organizations made it possible to gradually define the methods that are briefly described below. From the beginning, IPSN played a guiding role, defining approaches that were adopted and developed by EDF.

In general, at EDF (locally and in the centralized corporate services – Corporate Operations Engineering Support) and at IRSN, today's methods are generally based on the same principles:

- first a review of significant events (generally a collaborative task shared by analysis units) leads to a selection of events that deserve analysis. Whether performed by EDF (at the corporate level) or IRSN, this examination takes place weekly;
- the selected significant events are analysed, possibly in depth. Whatever the type of analysis, it is important to look for the root causes of these events, beyond those immediately identifiable;
- the analyses are then 'extended' or 'generalized' by examining how the events would have happened in less favourable circumstances or in combination with other failures. This is to determine the potential consequences of these events and, especially, whether they could have led to core melt or significant releases, the goal being to define priorities for implementing corrective measures decided upon as part of operating experience feedback. The 'extension' may also lead to asking what would have happened if the same event had occurred in another reactor of the nuclear power plant fleet.

In addition, IRSN holds a specific monthly internal meeting during which it examines all events that have occurred over the previous month (the ‘deviation meeting’). This examination serves to detect any operating deviations or equipment anomalies.

As part of the extension of analyses, the search for precursors using probabilistic methods was developed starting in the 1990s, by both EDF and IPSN, and later by IRSN. This type of analysis is based on Level 1 probabilistic safety assessments (PSAs) and is presented in Section 14.5.3.1. It involves quantifying the increased risk of core melt induced by the event, once this event occurs (probability of 1). Quantifying the difference separating an event that actually happened from a core-melt accident sheds insight on the severity of the event, which can then be quantified by the increase in the probability of core melt[645]. This represents the conditional probability of core damage during the event under consideration. The events for which the increase in core melt probability is greater than 10^{-6} are called ‘precursors’. Among these events, those for which the increase in core-melt probability is greater than 10^{-4} receive special attention. Since the middle of the 1990s, EDF (centralized corporate services) and IRSN have been developing ‘precursor programmes’ based on their own probabilistic models, which they compare regularly. The objective of this development project is to elucidate:

- the prioritization of events to be addressed,
- the evaluation of how relevant the operating experience feedback actions are,
- the enrichment of safety culture, by highlighting the most important measures or those whose importance has been underestimated, as well as high-risk operating situations and transients,
- the validation and improvement of PSA models in terms of sequences and data.

Since 2015, IRSN, when analysing the potential consequences of significant events and conducting precursor analyses, has taken into account the actual state of facilities, pointing out, for example, nonconformities that have not yet been addressed, emphasizing the need to rapidly remedy these nonconformities in certain cases. EDF was asked to develop a similar approach.

Some of the important aspects of significant-event analyses are discussed below – with a special focus on analyses conducted by IRSN.

▶ Collective examination of events

Within IRSN, an engineer is specifically assigned to monitoring a set of plant units (generally two units). To take advantage of the standardization of French pressurized water reactors, all significant events relating to these units are brought to the attention of these engineers through the distribution of event reports.

[645] This expression is used by IRSN, whereas EDF generally uses the expression ‘potential risk index’.

As indicated above, all significant events are mentioned at the weekly meetings, during which those considered the most important are selected. At these meetings, the engineers also note the most relevant recent events and exchange available information on events in other countries. In this way, each engineer is kept informed of what is happening across the French fleet, as well as important events in other countries.

The work method is similar in the centralized corporate services of EDF.

▶ Choice of in-depth analyses

During weekly meetings, the significant events that deserve in-depth analysis are selected. The selection criteria are not formalized, but the general principles applied usual lead to the selection of the following type of events:

- events close to the accident operating conditions taken into account for design and that have an estimated frequency below 10^{-2} per year and per unit, or are liable to lead to such accident conditions, possibly in other operating conditions,
- events not covered by the incidents or accidents used for facility design,
- combinations of failures in systems important to safety, whether they are due to random failures, common-mode failures or interaction between systems, as well as combinations of errors,
- events that reveal errors resulting from a lack of knowledge of facility behaviour or nuclear safety requirements.

This means that design rules and criteria are thus systematically referred to, albeit implicitly, making it possible to assess both the significance of the event and the validity of design rules. The engineers must therefore have appropriate knowledge or seek out the advice of specialists.

Since the first probabilistic safety assessments conducted for French nuclear power reactors, PSA specialists have contributed to facility monitoring. This approach identifies events involving failures that could significantly affect the probability of core melt, possibly in other operating conditions as well. This points to an important connection between two areas of safety analysis.

▶ In-depth analyses

In-depth analyses can lead to significant and long discussions or studies, nationally or internationally. Aside from the Three Mile Island, Chernobyl, and Fukushima Daiichi accidents, examples include some of the significant events described in the following chapters (partial flooding of the Blayais nuclear power plant site at the end of December 1999 – this analysis is discussed in detail in Section 24.1 –, an oil leak in a reactor coolant pump on Unit 2 at the Penly nuclear power plant in April 2012, etc.).

Within EDF, an in-depth analysis method was gradually developed and systematically applied by facilities, which gradually improved significant-event reports. The

National Guide to In-depth Analysis of Events stipulates a specific formalism as well as the method to be used on site by each operator, whose task is to[646]:

- "reconstruct what happened in detail,
- identify what was expected relative to the baseline requirements (safety analysis report, general operating rules, quality manual, etc.),
- analyse what could have happened (potential consequences),
- determine the root causes of the event,
- choose an approach to deal with the event depending on the relevant issues so as to avoid recurrence."

The in-depth analyses conducted by IRSN generally use a similar structure, discussed below, in which special attention is given to the event's impact on defence in depth – more specifically, to the deterministic safety assessment regarding:

- the representativeness of the initiating events used in the safety demonstration,
- the appropriateness of the choice of operating conditions,
- the exhaustiveness and representativeness of the hazards selected,
- concerning accident study, the time periods and possibilities for implementing operating procedures, the behaviour of confinement barriers, the qualification of equipment,
- the evaluation of the radiological consequences of accidents.

The 'zero point' of any significant-event analysis always involves gathering the information required to understand the initial state of the facility, the event sequence, the safety functions that may have been compromised, the behaviour of operators and equipment, the actual consequences, and any similar events.

Whatever the quality of the event reports submitted by the operator, it is generally necessary to supplement them with information gathered through direct contact (or contact with the centralized corporate services of EDF), which often involves visiting the concerned facilities and seeing equipment. One best practice is for IRSN to document its understanding of the event. In this way IRSN can share its analysis with the operator, avoiding a situation where the operator perceives the process as an investigation.

The actual consequences and any possibilities that could lead to degradation of equipment, systems and safety functions must be examined.

The root causes of the event should be sought by moving as far back as possible through the various branches of the cause-tree prepared for the event, covering not only the equipment, but also procedures and human behaviour. This involves

[646] See Section 2.2.3.2.2 in Chapter IV of the *Mémento sûreté en exploitation*, (Memento on Operational Nuclear Safety), EDF, 2016 edition.

distinguishing between what is specific to the facility and what could occur in other reactors. The possible causes of common-mode failures must be identified.

It is useful to apply the identified root causes to other equipment, systems, operating states or situations, to ensure that they could not initiate a sequence of different and potentially severe consequences. For example, if the leak in a check valve of a compressed air system caused an event despite the fact that this valve did not have a singular defect, all the valves of the same type associated with safety functions must be identified and the possible consequences of their failure examined. More broadly, failures in document quality or management or in work organization and scheduling must lead to examining these same aspects for other equivalent activities.

Special attention must be given to worker response by:

- identifying human actions and interactions (such as available documents, consulted documents),
- reviewing the success of procedures and operator response times.

The next step in the analysis is to look for similar events of the same type as well as any precursors or warning signs. Obviously, an in-depth analysis of a significant event must not be isolated from the general context of other events in the French nuclear power plant fleet and elsewhere in the world. It is also clear that similarities must be sought in a very broad manner. This applies to events involving similar scenarios as well as those involving the same equipment, human or organizational causes.

These associations are essential to correctly assess the lessons to be learned from a significant event and consequently extrapolate these lessons to a more general context.

Simple corrective measures, such as guidelines to prevent scenarios with more significant consequences following an initiating event of the same type as the one observed, can generally be implemented quickly and at low cost. EDF and IRSN can easily agree on this type of measure. The discussions are more difficult if facility modifications are considered necessary, especially if they must be applied on a widespread basis to other equipment items, to many plant units or if they are costly.

IRSN's analysis always includes assessing the corrective actions taken by the operator in terms of equipment, organization and documentation. If necessary, it may lead to defining proposals calling for additional actions, which must be discussed with the operator before IRSN's analysis-based opinion is submitted to ASN.

These exchanges on technical issues contribute to advancing reflection on nuclear safety. It does not limit IRSN's independence as long as the points of agreement and disagreement are clearly defined and are supported by pertinent arguments.

Like all reports prepared by IRSN, an in-depth significant-event analysis report culminates with conclusions and recommendations that may be used by ASN. The in-depth significant-event analysis reports prepared by IRSN are made public.

It is important to note that IRSN's role is to issue an opinion on the acceptability of the operator's proposals. The Institute is not in a position to prescribe technical solutions. The operator remains responsible for making such decisions.

▶ Milestones for OPEX, general assessments, overall analyses and targeted analyses

To obtain an authorization for the first fuel loading of a reactor, EDF must submit a file to ASN that includes the results of the startup tests. It is during these tests that the first operating experience feedback may emerge, in terms of checking that the facility is built correctly and validating its design. The first years of reactor operation with its operating crews may also offer useful lessons involving operating practices, beginner's mistakes or particular events that occurred and how they were addressed.

Operating experience feedback pertaining to events occurring on reactors in the French nuclear power plant fleet are then analysed once every three years. These analyses, performed by IRSN in collaboration with EDF, are presented to ASN's Advisory Committee on Reactors.

Specific reviews on sensitive subjects may also be planned, for example, following recurrent events or significant incidents or accidents. This was the case after the accidents in the Chernobyl and Fukushima Daiichi nuclear power plants. It was important to rapidly examine the relevant lessons for the French nuclear power plant fleet. In addition, recurrent or multiple events in parts of nuclear safety systems may lead to reviewing safety functions on an overall basis (design, construction, periodic inspections and tests, maintenance, etc.). Thus, in 2008, subsequent to many events[647] (including compliance deviations) involving water recirculation in accident conditions, ASN asked EDF to review this safety function to determine its actual availability, which led the operator to define a schedule for addressing the deviations, along with corrective measures in the meantime.

For each of these situations, IRSN's expert assessment can lead to recommendations and then requests issued by ASN to EDF.

Furthermore, IRSN prepares reports on its position regarding the state of the French nuclear power plant fleet (for the past year), which are made public. Organizations that receive these reports include EDF, ASN, ANCCLI (National Association of Local Information Committees and Commissions) and the Local Information Commissions. This type of report is used to review actions taken and changes made by EDF following the events that have occurred. It provides additional information to the public which, in certain cases, is only informed that certain events have occurred.

Aside from the generic failures and anomalies in some reactor components that may appear over time, the operating experience feedback analyses highlight trends (such as a change in the number of significant events), best practices or sensitive

[647] About 200 events were considered relevant between 1998 and 2008.

aspects to which EDF must give particular attention, whether they involve nuclear safety or radiation protection. These sensitive aspects include:

- the quality of maintenance operations (preparation sometimes insufficient, inappropriate actions taken on equipment, incorrect implementation, inadequate inspection, insufficient monitoring of subcontracted activities),
- the use of operating 'baselines' by plant personnel and the frequent changes to these baselines, complicating the manner in which they are applied in operating documents,
- the application of radiation protection principles.

There are sometimes significant disparities between facilities.

But it should be emphasized that changes in the number of significant events are not directly related to changes in the level of nuclear safety or radiation protection at facilities. These events reflect malfunctions that must be analysed and understood, in the context of the operating experience feedback process, to define corrective actions that contribute to improving nuclear safety and radiation protection. Therefore, this book does not discuss specific indicators or trends – which can be found, for example, in the annual reports of IRSN. Instead, the choice was made to focus the following three chapters on some of the key significant events that have occurred on reactors in the French nuclear power plant fleet, how they were analysed, what lessons were learned and what concrete measures were taken in the facilities.

To conclude this chapter on the rules and practices of operating experience feedback, it is useful to mention a specific approach that IRSN has used since 1997, aimed at learning other relevant lessons from significant events. This is the 'Recuperare' approach. This innovative approach uses a database in which significant events are standardized in a specific way, which not only tracks any equipment failures or operator errors, but also how they were detected and the resulting situations corrected[648] by these operators or other members of the operating crew. This database highlights certain overall trends, while pointing out differences between the various sites. It also provides information on recovery time that can be used in probabilistic safety assessments.

Using the Recuperare approach focuses attention on:

- the annual frequency of human errors and technical failures and the context in which they occur,
- potential latency of equipment failures and the latency period before setting into operation equipment involved in the failure,
- dependency between the factors related to errors and those related to recovery,

[648] In French, the verb meaning 'recover' is '*récupérer*', hence the 'Recuperare' approach for recovering from situations caused by faults or for event management.

- time taken by operators to detect problems and correct them (response time). This is a particularly important point because the consequences of an event can be more or less severe depending on the response time.

To structure[649] significant events in the database associated with the Recuperare approach, six types or families have been adopted:

- Type A: latent fault discovered and corrected before startup of the relevant system.
- Type B: latent fault discovered and corrected after startup of the relevant system.
- Type C: fault revealed once the system was already in service.
- Type D: combination of faults (for example, repetition of the same error, fault that occurs while recovering from an initial fault, strategy error resulting in various inappropriate actions).
- Type O: organizational failure without direct consequences in the facility.
- Type R: radiation protection fault.

The results of the Recuperare approach regularly add new information to the general overview of significant events and team performance during these events, as well as any changes from one year to another.

The Recuperare approach has also shown that 50% of significant events belong to Family C, that recovery is generally more efficient and rapid during night shifts, that the latency periods can be very brief or may last up to 50 days, and that fault detection time can take as long as 10 days. The approach has also shown that the most relevant significant events for nuclear safety are those for which detection and recovery were particularly slow.

Some of the lessons learned from the Recuperare approach have been discussed with EDF, more specifically during the periodic meetings of the Advisory Committee for Reactors focused on operating experience feedback. For example, in 2001, EDF shared IPSN's observation on the persistence of a relatively high number of alarms that were not detected for more than several hours. This led the operator to take measures to shelter reactor control room personnel from unnecessary disruptions.

[649] Structuring is achieved mainly based on significant-event reports.

Chapter 22
Operating Experience from Events Attributable to Shortcomings in Initial Reactor Design or the Quality of Maintenance

The rules and practices adopted for analysis of events occurring in French nuclear power plants, with a view to learning lessons from them in order to avoid their recurrence and improve facility safety, are discussed in Chapter 21.

In France, no event leading to substantial release of radioactive substances has occurred during the operation of pressurized water reactors. Inadvertent releases have nonetheless occurred, for example, following malfunctions of relief valves on radioactive effluent storage tanks. However, several significant events that have occurred in France must be considered as precursors of more serious situations, although they do not systematically involve accidents causing major reactor core damage. Based on criteria in the 'precursor programme' (see Chapter 21), about 15 such events are recorded every year throughout the entire fleet.

On the basis of a selection of noteworthy events[650] grouped into categories, including some events considered to be precursors of core damage accidents[651], this

[650] See also Chapter V, Section 2.2, of the EDF document *Mémento sûreté nucléaire en exploitation* (Memento on Operational Nuclear Safety), 2016 edition, in which other events are described.

[651] Although some of them occurred before the precursors programme was implemented.

chapter and the next two chapters examine some of the issues raised in the context of analysis of these events, with the measures taken by Électricité de France (EDF) in response to these issues.

For each event category, the course of events is described first, with the actions taken by the facility operator to mitigate the consequences, then the lessons learned are summarized for the facility in question and more broadly for all nuclear power plants.

Two categories of significant events that occurred over the first decades of operation of the French nuclear power reactors are covered specifically in this chapter, the first category providing evidence of a weakness in reactor design, entailing an unacceptable increase in the probability of core melt in their outage states, and the second category pointing to the inadequate quality of maintenance operations. At the time, these events led to strong reactions by both EDF and safety organizations.

Note that several events involving anomalies concerning equipment (including fuel rods, control rods, reactor vessels, pressurizers, system pipes, steam generators, etc.), are described in chapters 26 and 28.

22.1. Events attributable to design shortcomings: core cooling deficiencies when reactor is shut down with water level in mid-loop operating range of the residual heat removal system (RHRS)

It is often difficult to determine rapidly and definitively the corrective measures necessary to avoid the recurrence of an event that has occurred and undergone detailed analysis. A characteristic example concerns the risk of core cooling interruption when the reactor is shut down with the reactor coolant system partially drained to the level of the loop pipes. Events occurred in these conditions in France in 1979 and 1980, and in many countries operating similar types of water-cooled reactor. In particular, these events provided evidence of a significant risk of core melt in the shutdown states, necessitating additional prevention measures.

The layout of the components in a French 1300 MWe nuclear power reactor is shown in Figure 22.1. Partial draining of the reactor coolant system to a level slightly below the highest level of the pipes in the system can be used to drain the steam generators and sweep the system with air before opening the reactor vessel. Sweeping the pipes limits the subsequent radiological constraints for personnel. Moreover, to allow work by personnel in the steam generator channel heads and inspection of the steam generator tubes when the core is not unloaded, the connections between the channel heads and the reactor coolant system loops must be blocked by nozzle dams. As the nozzle dams are installed manually, the channel heads must be drained and a sufficient level difference obtained to avoid any inadvertent increase in the water level during the operation. The water level is equivalent to 70% filling of the hot and cold legs of the reactor coolant system, below the level necessary for operations required prior to opening the vessel.

The residual heat removal system (RHRS), which cools the reactor core in these configurations, is connected to the reactor coolant system at the bottom of the pipes. As the water seal is relatively small, a flow rate that is too high or a water level that is too low could result in vortex generation with air suction. The pumps could then lose prime, interrupting proper cooling of the core. As these difficulties had not been identified when the reactor units were designed, the only available level measurement function was imprecise and unreliable.

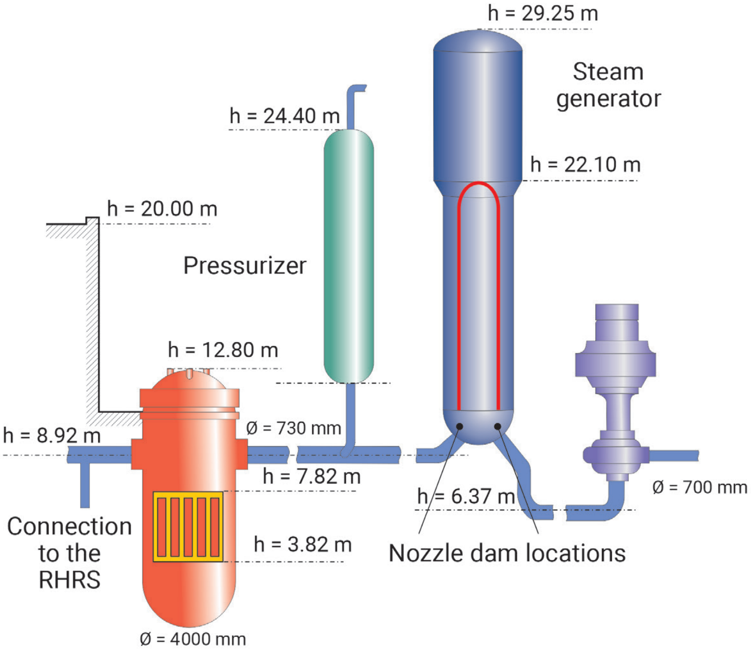


Figure 22.1. Layout of components in a 1300 MWe reactor. IRSN.

▶ Potential consequences

In the configurations considered, the reactor coolant system of a 900 MWe reactor contains about 70 m^3 of water, but only the 45 m^3 of water contained in the reactor core zone and above it must be taken into account for the time-to-boiling. After three days of shutdown at the end of the cycle, decay heat released by the core is about 12 MW. Around 15 min without cooling is long enough for the temperature of this volume of water to increase from 40°C to 100°C. Core uncovery then begins when the 12.5 m^3 of water above the fuel assemblies have been vaporized, which only takes another 40 min. These time intervals are longer when decay heat is lower, but it should be noted that, after one month, the decay heat is still 4.5 MW, which gives time intervals of 40 min to boiling and a total of 146 min to the beginning of core uncovery.

The actual times are in fact a little longer, due to the heat capacity of the metal core structures.

Boiling of the water would result in contaminated vapour being transferred into the reactor building, where personnel could be present. Fuel uncovery would cause cladding rupture, leading to much more serious radiological consequences for reactor building personnel, and even outside the reactor building if it did not provide adequate confinement.

The first event of this type analysed in detail (by IPSN) occurred at Unit 1 of the Blayais nuclear power plant on 6 May 1983 when the reactor pool was drained in order to reinstall the reactor vessel head, after refuelling. Inadvertent isolation of the vessel water level measurement sensor, misleading the operators, resulted in an excessive water level drop, uncovery of the residual heat removal system water intake, loss of core cooling lasting 2 h, and a 20°C increase in the reactor coolant system water temperature. The reactor had been shut down for 93 days, and decay heat dissipation was about 1.4 MW.

▶ Corrective measures taken

The following actions were taken by EDF after this event:

– modification of the reactor vessel water level measuring instruments and systematic verification of its presence during line-up,

– modification of the draining procedure, with draining flow rate limitation,

– clarification of the corresponding procedures,

– information sent to the other facilities and training of the operators.

In late 1983, IPSN suggested that more reliable instruments be installed for measuring the reactor coolant system water level and temperature. These suggestions were taken up by the Advisory Committee for Reactors and were requested by the Central Service for the Safety of Nuclear Installations (precursor of the French Nuclear Safety Authority – ASN) in 1987.

As the same type of event had occurred several times in the USA, the topic was discussed in a working group set up by the Nuclear Energy Agency of the Organisation for Economic Cooperation and Development (OECD/NEA) in 1985 to examine the safety system failures declared to the Incident Reporting System (IRS). The working group's report, issued in November 1986, identified 19 IRS reports on incidents involving dropping reactor coolant level in reactor shutdown states, with some of these reports covering several events. The suggested corrective measures, necessarily very general in this context given the wide diversity of facilities, confirmed the measures described above.

Other events involving reactor cooling in a shutdown or outage state occurred in French plant units over the years following the 1983 incident. Core cooling at Unit 4 of the Blayais nuclear power plant was lost for 25 min in 1985, heating the reactor coolant system water by 25°C. In 1987, the residual heat removal system pump in service at Unit 1 of the Cruas-Meysse nuclear power plant operated for 3.5 h in abnormal conditions without degradation or loss of reactor core cooling.

These events led EDF to reinforce preventive measures by making the safety injection water reserve available on standby to provide makeup water to the reactor coolant system and, in 1988, by installing a second water level measuring instrument using ultrasound, a different technology from the first instrument.

During this same period, several more events of the same type occurred in reactors in the USA (San Onofre Unit 2 in 1986, Diablo Canyon Unit 2 in 1987). Following these events, the U.S. NRC addressed a generic letter to facility operators calling their attention to the corresponding risks.

This letter and the first results of probabilistic studies carried out in France, which showed the significant proportion of shutdown situations in the calculated total frequency of core melt[652], led EDF to define requirements in 1989 relevant to cold shutdown states for work on reactors, which were added to the operational limits and conditions.

These additional requirements reinforced defence in depth:

– improvement of prevention by:

    - redundancy and diversification of vessel water level measurement methods,
    - improved draining procedure,
    - availability of two residual heat removal system trains and two emergency backup options for the system, either by a steam generator when the reactor coolant system is closed and filled with water, or by the fuel pool cooling system otherwise,
    - setting a minimum time before reactor coolant system opening to ensure a response time of 1 h before the beginning of fuel uncovery,
    - opening the pressurizer manway before any other reactor coolant system opening to avoid core draining by pressure increase in the event of loss of cooling,
    - strict limitation of work on the systems connected to the reactor coolant system or to the residual heat removal system,

[652] These studies showed a total core melt frequency of 5×10^{-5} per year and per reactor for the 900 MWe series reactors and 10^{-5} for the 1300 MWe series reactors, the contribution of shutdown states representing more than 30% for 900 MWe reactors and more than 50% for 1300 MWe reactors. Furthermore, the scenarios of heterogeneous dilution and vortex in the RHRS were not included because measures had to be taken to resolve the corresponding issues (the vortex scenarios alone had been estimated to contribute a risk of about 10^{-5} per year and per reactor).

- improvement of monitoring by:
    - better tracking of the residual heat removal system operating parameters (measurements of temperature, pump current draw, flow rate, pressure),
    - establishing a hold point before lowering the reactor coolant system water level below the low level of the vessel head; the hold point must not be released until all the above measurements have been checked;
- improvement of mitigation in the event of an abnormal situation by:
    - availability of two gravity-driven water makeup lines from the safety injection water tank and the spent fuel pool,
    - maintaining confinement,
    - countermeasures on standby in the event of total loss of electrical power,
    - incident procedures for residual heat removal system water makeup and emergency supply.

In 1990, the DSIN (Nuclear Installations Safety Directorate) decided that any transition of the residual heat removal system to mid-loop operation conditions must be subject to prior DSIN agreement.

Following the publication in 1990 of the results of the French probabilistic studies, which underlined in particular the importance of the estimated frequency of core melt in these unusual configurations, EDF decided to conduct a complete programme of studies and tests on this topic. The programme included an analysis of all French and international operating experience feedback, additional thermal-hydraulics calculations to determine the RHRS operating margins with respect to cavitation and vortex formation, and the development of additional measuring instruments. The results of these studies were reported to safety organizations in late 1994. Of the proposed additional equipment, the incorporation of an automatic water makeup system for the reactor coolant system was approved.

However, despite the measures introduced, further events occurred. A particularly notable event occurred on 29 January 1994 at the Bugey nuclear power plant, during which a lack of precision in operating documents led to the establishment and maintenance of a vortex situation lasting more than 8 h. Core cooling, however, was not affected. Two successive shift crews were involved in this situation, and the safety engineer did not detect the anomaly when in the control room. This event motivated initiation of the 'sensitive transients' approach within EDF, implemented for all its nuclear power plants by a specific directive (DI 118), updated regularly (see Section 25.2.1). This approach emphasizes the importance of preparing this activity in advance and preparing personnel to control the transient, calling for analysis or review of risks, task allocation and organization of monitoring in the control room.

22.2. Recurrent loss of safety function events related to maintenance operations – Lessons learned

22.2.1. Events

Between January 1986 and December 1989, several events related to maintenance operations, involving complete loss of a protection function or an engineered safety function, occurred in France and in other countries. Although partial loss of a safety function is considered in design studies, simultaneous loss of identical components fulfilling the same function or belonging to redundant trains is abnormal and must remain exceptional, despite the implementation of countermeasures at the facilities (additional components and procedures).

A noteworthy example outside of France is the event that occurred in 1987 at the Philippsburg nuclear power plant in Germany (near Karlsruhe). During the annual refuelling outage, following the periodic test conducted to check the reactor protection system threshold settings, the facility operator observed that all the emergency diesel generators had been disconnected from the reactor protection system. The startup and reconnection sequences of the emergency actuators had consequently been rendered inoperative on four redundant trains for some 15 h. As soon as this anomaly was discovered, the generators were reconnected to the reactor protection system. The causes of the event were identified as resulting from both poor organization and inappropriate procedures. The reactor coolant system was drained to the three-quarters loop level (water level in the mid-loop operation range of the residual heat removal system) in preparation for reactor vessel head opening. In the event of loss of off-site electrical power, the automatic emergency supply to the actuators necessary for cooling would not have been available, which would have led to relatively rapid heating of the reactor coolant system.

The following events were the most characteristic in France.

- In May 1988, degradation of the raw water filtration function at the Cruas-Meysse nuclear power plant.

  During a daily field inspection, tears were observed on the four drum filters of the reactor condenser cooling system. This system filters the raw water, used as the heat sink, downstream of the water intake grilles. This means that it is one of the links in the core cooling chain. Investigation by the facility operator showed that the origin of the tears dated back to five months before the partial unavailability of the filtration function was discovered. The observed tears were caused by a falling foreign object left behind after engineering changes had been made. There were no real consequences of the unavailability, as operation of the reactor units was not disturbed and fouling of the component cooling water system heat exchangers did not increase unusually during this period. The tears were small enough to not significantly alter the quality of the cooling water. The consequences would have been more serious if larger tears had led to degradation of the quality of the filtered water, particularly in periods when the river water is heavily loaded with debris (dead leaves, silt due to thunderstorms). The risk would then have been fouling or plugging of the component cooling water system pipes or heat exchangers and consequent loss of cooling to the chemical and volume control system and the spent fuel pool cooling and purification system (however, this accident situation had been taken into account in the context of the beyond-design-basis procedures).

- In May 1988, simultaneous loss of both trains of the component cooling water system at Unit B3 of the Chinon nuclear power plant.

  The event occurred during a reactor refuelling outage, with the spent fuel located in the fuel building. The heat exchangers on the two trains of the containment spray system were isolated and drained on the secondary side (CCWS) in preparation for carrying out periodic tests. One train of the component cooling water system was in service. When the heat exchangers were returned to service, a low water level was detected in both trains of the system, leading the shift crew to force the shutdown of all the pumps, resulting in total loss of the component cooling function for 38 min. Spent fuel pool cooling was shut down even though the core fuel assemblies were in the fuel building. However, the thermal inertia of the pool was such that the increase in the pool water temperature was negligible.

- In August 1989, common-mode degradation of the reactor coolant system overpressure protection at Unit 1 of the Gravelines nuclear power plant.

  Reactor coolant system overpressure protection is provided by three tandems of pilot-operated relief valves (SEBIM^{TM}). Each tandem comprises a pressure relief or safety relief valve associated with an isolation valve located downstream. Each of these relief valves is actuated by the pressure value transmitted over impulse lines to a control unit. Abnormal restriction of the supply line to the control unit of the three safety relief valves of the reactor coolant system at Unit 1 of the Gravelines nuclear power plant was detected in August 1989, when the relief valve settings were checked during a refuelling outage. The event was the consequence of an assembly error (fastening with solid screws instead of drilled screws) during the previous outage in 1988, when it was necessary to disconnect and reconnect the impulse lines for the periodic tests conducted to check the relief valve settings. On completion of the work on the control unit, considered as a low-scale operation, the relief valves were not tested to ensure they functioned correctly (and procedures did not require checking these devices). If valve operation had been necessary, this anomaly could have caused them to open later than expected and at higher pressure than specified. However, the relief valves could still be opened by manually operating the bleed solenoid valve. The event had no immediate consequences insofar as the relief valves were not actuated during the period considered from June 1988 to August 1989.

  As soon as the event was detected, EDF rapidly made sure that the impulse lines in all the other nuclear power reactors were secured using drilled screws.

It appears that it was mainly the presumed insignificant character of the operation that explained the fastening error at the origin of the incident. An important lesson learned from this event is the common-mode risk associated with work done simultaneously on identical components that are redundant or taking part in the same function.

- In August 1989, unavailability of an engineered safety system at Unit 1 of the Dampierre-en-Burly nuclear power plant.

  On 1 August 1989, the facility operator discovered closure plates in the reactor penetrations for the containment air renewal system blower and hydrogen recombination. These (temporary) closure plates had been installed on both trains of the system for the containment leak test during the previous refuelling outage in September 1988. In the event of a loss-of-coolant accident (LOCA), these plates would have rendered hydrogen recombination ineffective. A similar event had occurred in April 1987 at units 2 and 3 of the Bugey nuclear power plant. This oversight illustrates the risks associated with temporary components used by maintenance personnel.

Following these events and looking beyond their analysis and the corrective measures introduced, a more general review of reactor outages was undertaken in 1989 by EDF, at the request of the Minister of Industry and Regional Development and the secretary of state reporting to the Prime Minister, responsible for the prevention of major technological and natural risks, who asked "that a critical analysis be undertaken within the corporation regarding all organizational measures and resources implemented to ensure the quality of maintenance operations"[653]. For this critical analysis[654], safety organizations examined the choice of the lines of investigation, the progress of discussions, and the decisions taken and implemented at its facilities by EDF. The topic was also discussed at two meetings of the French Consultative Council for Nuclear Safety and Information (*Conseil supérieur de la sûreté et de l'information nucléaires*, CSSIN) in 1990 and in 1991, which observed progress of the case on maintenance improvement at EDF.

Certain types of event were identified in the analysis. One type involves line-up of the water level sensors in the pressurizers, which was an issue in several events of this type that occurred in 1989 and 1990:

- In October 1989, the pressurizer heaters at Unit 2 of the Flamanville nuclear power plant were damaged.

  Pressurization of the reactor coolant system requires the formation of a steam bubble in the pressurizer. The bubble is formed by switching on electric heaters to boil the water. When Flamanville nuclear power plant Unit 2 was restarted after refuelling, an error in the valve line-up of several pressurizer water level

[653] Letter CAB no. 65221 M2 of 19 September 1989.

[654] Which was presented in a report (the 'Noc Report', named after its coordinator, Bernard Noc, at the time head of the nuclear safety mission within EDF).

sensors resulted in uncovery of the heaters during bubble formation. Since the isolation valve remained closed on the low impulse line tap for four out of the five level sensors (see the next Focus feature on valve RCP 81 VP), the operators did not observe any anomalies during initial filling of the pressurizer. Consequently, when the reactor coolant system was pressurized, four sensors indicated a maximum level while the bubble was being formed. The only sensor in service was ignored, as a malfunction was suspected because of its different behaviour compared with the other four. Pressurizer draining thus continued until the heaters were uncovered, resulting in their destruction by overheating. The shift crew then realized that an abnormal situation was developing, and proceeded with operations to refill the pressurizer. Reactor restart was interrupted, and the reactor was brought to the cold shutdown state for the necessary repairs. Investigation showed that 65 heaters that had operated while uncovered had been damaged. This event, which was not likely to lead to core damage, is significant for the lessons to be learned: its cause is related to conducting work simultaneously on several redundant components of the same function. One important observation is that the event developed because operators trusted four false level indications without methodically cross-checking against other sources of information available in the control room. There is a similarity, at least in this respect, with the TMI accident, in which the operator did not realize that a pressurizer letdown valve was still open because a false indication showed that it was closed.

#FOCUS

Water level measurement in pressurizers (1989 event)

To help understand the description of the 1989 event above, the principle of water level measurements in pressurizers is described briefly below (description corresponding to the state of the French nuclear power reactors in 1989).

The water level in the pressurizer is measured by differential sensors that measure the weight of a water column of about 10 m from eight nozzles on the pressurizer casing (Figure 22.2). These nozzles also feed the pressure sensors; each nozzle has a process interface valve for isolating the measuring system, and this valve is considered to be part of the reactor coolant system. These valves each bear a specific identification number given on the drawings and used in the procedures. Their operation comes under the responsibility of the Operations department.

Each level sensor has a separator, drains, test instruments, and seven valves considered to be part of the instrumentation itself; however, they are located relatively far away from the sensor, at the level of the two nozzles, which are separated vertically by a distance of 11.5 m, either near the pressurizer or beyond the 'anti-projectile' barrier protecting it. They can be accessed from various platforms provided over a height of about 12 m.

These valves do not have unique identification numbers, but are identified locally only as V1 to V7, without identification of the corresponding sensor, and are generally not shown on the drawings available to the Operations Department. Their operation is the responsibility of the Automation Department.

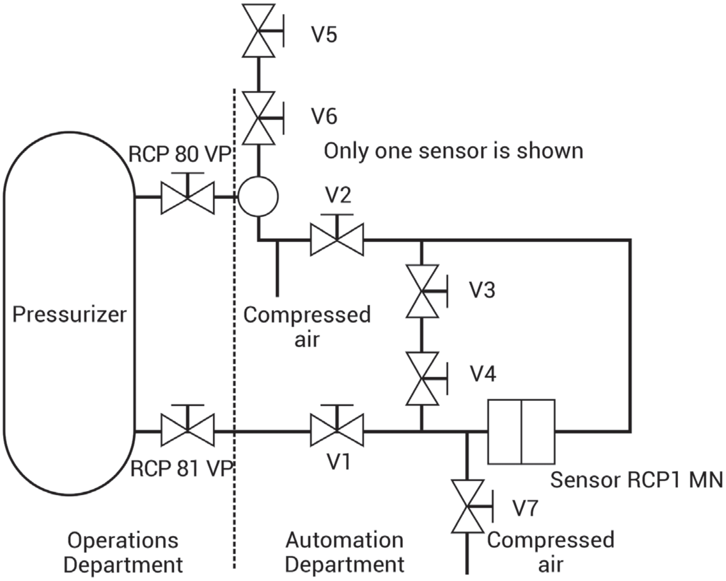


Figure 22.2. Schematic diagram of the pressurizer water level measurement sensors. IRSN.

- In September 1990, the six steam flow rate measurement sensors were unavailable at Unit 1 of the Dampierre-en-Burly facility.

  On startup of this reactor after its first ten-yearly outage, when connecting to the electricity grid, with the reactor at 15% of its nominal power, the operators noticed that there was no change in the steam flow rates: all the steam flow rate sensors were still isolated because requalification had not been carried out completely. The reactor was immediately returned to hot standby to reset the necessary parameters and restore sensor operation. From the safety point of view, the function that triggers the safety injection system via the steam flow rate sensors was unavailable on all three steam generators of the reactor. However, the other protection systems would have fulfilled their function in the event of a steam line break, including triggering of the safety injection system by detection of high differential pressure between steam lines or low-low pressure in the pressurizer. The origin of this event was incomplete requalification following successive errors explained by the manner in which tasks and responsibilities had been broken down and assigned to personnel, both by the contractor (Framatome) and by the facility operator. It should nevertheless be emphasized that functional requalification of the sensors had been planned during the reactor power ramp-up; planned, but too late in the process.

- In March 1990, pressurizer water level measurement sensors were isolated at Unit 2 of the Cruas-Meysse nuclear power plant.

  When the incident occurred, the reactor had been shut down for 15 days for unscheduled work on a steam generator. During the transition from the maintenance cold shutdown state to the normal cold shutdown state, the facility operator proceeded with vacuum refill of the reactor coolant system before the system had been completely refilled with water. The reactor pressurizer water level sensors had been replaced in 1989 by sensors qualified for accident conditions. Since the new sensors were not designed to withstand negative pressures, the operating procedure specific to the facility had been changed. An amendment to the procedure required that these sensors be isolated using the 'level sensor valves' during the vacuum refill, without further details. Closing the process interface valves led to isolation of another sensor used to monitor the water level as the reactor coolant system was being filled. Consequently, the level had to be monitored locally. The water level sensor, however, based on a different technology, did not need to be isolated. The valves associated with the relevant pressurizer sensors should have been closed, not the process interface valves. The text of the procedure did not specify who should carry out this isolation, or which valves should be operated and how. The author and reviewer of the procedure did not have sufficiently thorough knowledge of the details of the measuring systems. This resulted in different inconsistent actions taken on valves – not identified locally – by successive shift crews. In the end, it was three days later, after the reactor coolant system was filled with water and when the bubble was formed in the pressurizer, that an operator diagnosed the abnormal indications provided by the sensors and requested a local check. This revealed line-up errors and, after they were corrected, reactor startup was resumed.

- In November 1990, isolation of pressurizer water level measurement sensors at Unit 4 of the Gravelines nuclear power plant.

  The event occurred when the reactor was in the restart phase after the annual refuelling outage. Before the reactor coolant system was vacuum refilled, the pressurizer water level sensors were isolated. As at Unit 2 of the Cruas-Meysse nuclear power plant, the sensors had been replaced in 1989 by sensors qualified for accident conditions. It was the first time that the pressurizer water level sensors at Unit 4 of the Gravelines nuclear power plant were isolated before reactor coolant system vacuum refill. The valves associated with the sensors did not bear any identification markings. The automation technicians team job planner realized this and added a drawing on which the valves concerned were colour-coded. The sensors were isolated. The next day, the sensors had to be returned to service once the reactor coolant system had been filled. The workload of the automation technicians team that had isolated the sensors was particularly heavy that day, so the work was assigned to a different team than on the previous day. As was normal practice for returning a pressure sensor to service, the team opened the valves closest to the sensors. However, it did not know that the level measurement sensor systems are more complex, and only carried out part of the work. The line-up error was detected two days later, during the temperature increase for formation of the bubble in the pressurizer; it was corrected, and the restart operations were then resumed.

The corrective actions were as follows:

- marking the instrumentation valves of certain sensors,
- introduction of a sensor operation verification procedure by which sensor indications can be validated by operations or periodic tests,
- introduction of an additional check for sensors whose indications cannot be validated in normal operation,
- ensuring consistency of maintenance sheets at corporate level,
- instructions to the sites to identify the sensors to be checked during an unscheduled outage.

Another type of event concerned common-mode failures due to the use of unsuitable measuring and calibration instruments:

- In July 1988, incorrect calibration of the two pressurizer pressure measurement sensors in the Chooz A reactor.

  When the reactor was at 100% of its nominal power, unusual operations of the pressurizer letdown line isolation valves were observed. The facility operator decided to measure the reactor coolant system pressure using a previously verified reference sensor. This sensor indicated 136 bars instead of the expected 138 bars. This observation led the facility operator to implement cold shutdown of the reactor in order to remove, inspect and recalibrate the sensors in question. The subsequent checks revealed a difference of about +3 bars from the actual pressure. The event in question was caused by the use of inappropriate checking equipment. During the refuelling outage that had begun on 24 April 1987, all of these sensors had been removed and checked in a workshop using a calibration system of the required accuracy. However, because the unit outage had been extended, the facility operator decided to check the reactor coolant system pressure sensors again, before restarting the reactor in April 1988; to avoid removing the sensors and transporting them to the workshop, their settings were checked locally using a portable system whose calibration was subsequently found to be offset. Verification of the pressure gauge on the portable test pump showed a difference of +3 bars over its entire measuring range.

This event had no direct consequence on safety, as the protection and engineered safety systems affected by the sensors in question had not been activated. In terms of potential consequences, the pressure measurements used for control and operation of the protection systems and engineered safety actions were all offset by about +3 bars, which could result in delayed activation in response to a pressure drop. The estimates determined by the facility operator on the basis of the accident studies showed that the delay would be very short (roughly a few seconds). Furthermore, the margin-to-boiling was reduced by about 3 bars from the average value; the facility operator stressed that the actual reactor coolant system pressure remained above the value used in the accident studies (135.5 bars). It should nevertheless be noted that, had the difference been greater, the situation would no longer have been covered by the accident studies.

- In April 1989, incorrect setting of the steam generator safety relief valves at Unit 2 of the Tricastin nuclear power plant.

  The event was detected when the safety relief valves of the steam generators were tested to check their settings, with the reactor in hot shutdown. Analysis of the test results showed a setting error, dating from the previous outage (1988), related to the method used. The settings of two valves were respectively 1.2 and 1.4 bars below the low limit of the acceptability criterion. The underlying cause of this incident was the failure to take into account uncertainty in the steam generator pressure measurements according to the technology of the measuring instrument used. The measuring instrument used in 1988 was different from that required by the test procedure. The measurement error due to the instrument used was greater than the error taken into account in the procedure to define the tolerance interval, and this was not noticed by the test operator.

  The event had no direct consequence on facility safety. A setting that is too low can be considered penalizing in the event of steam generator tube rupture, as it may lead to early opening of the relief valves concerned, a risk of them jamming in the open position (the relief valves are not qualified for water transfer), and consequently more significant release to the atmosphere. However, in the case of the Tricastin Unit 2 event, the main steam relief train would have limited the pressure peaks and there would not have been an increase in release to the atmosphere if a relief valve opened. It should nevertheless be noted that, although no positive setting error was detected, a larger negative setting error would have had the potential consequence of inadvertent opening of one or more relief valves if their pressure setting had been below the pressure set point of the main steam relief train.

- In May 1990, incorrect settings on the four power level neutron source range channels at Unit 6 of the Gravelines nuclear power plant.

A periodic test of the power level neutron source range channels (SRC) of the reactor showed that the first SRC checked was out of tolerance. Subsequent verification of the test instrument showed that it did not comply with the manufacturer's specification. Compliance of the instrument was re-established, the test was repeated using the same instrument, and the result was within tolerance.

However, the validity of the periodic test using the same instrument on Unit 6, which led to adjustment of the settings of the unit's four power source range channels, had been compromised; the periodic test was repeated with a previously-checked compliant instrument and confirmed this assumption, leading to readjustment of all the settings for Unit 6. Operation with non-compliant settings lasted nine days.

The event had no direct consequence on safety. Assessment of the potential consequences of these incorrect settings showed that the margins available, for the core in place, with regard to the assumptions of the accident studies were sufficient to ensure that the safety of the reactor had not been called into question during this period.

- In November 1990, an out-of-specification value of the boron concentration in the three safety injection system accumulators at Unit 1 of the Dampierre-en-Burly nuclear power plant.

  During a periodic test, the plant chemists observed that the boron concentration was out of specification in all three accumulators of the reactor safety injection system: the measured concentration was 2560 ppm, whereas the concentration required by the specification was between 2325 ppm and 2475 ppm. The previous measurement had given a correct value, and there had been no water movement in the system in the meantime, so the facility operator checked the measurement channel of the analyzer used to determine the boron concentration. This showed that the concentration of the sodium hydroxide used for the determination was not the same as the concentration entered in the calculator memory. This error resulted in overestimation of the boron concentration value by about 5.6%. The error was corrected, but two other borated water tanks were shown to be out of specification. Boron adjustment by the facility operator resulted in a return to an acceptable value as required by the operational limits and conditions.

Other similar events can be mentioned:

- Following the loss of off-site power resulting from the electricity grid incident on 12 January 1987, Chinon nuclear power plant Unit 3 could not switch over to islanding because of an incorrect setting of the protection system, leading to premature turbine trip. The diesel generators that started up on source switch-over did not connect automatically to the emergency-supplied switchboards because the undervoltage protection relays were set to 0.6 Un (nominal voltage) instead of 0.7 Un. This setting error was due to a fault in the calibration bench used to set the relays. Moreover, this locally-produced bench was common to the entire site.

- In August 1987, when Unit 1 at the Nogent-sur-Seine nuclear power plant was in the pressure ramp-up phase at the beginning of pre-critical hot tests, with pressure being monitored in the control room on the four pressurizer pressure sensor indicators, closing of the SEBIM™ tandem isolating valves was inhibited at 140 bars instead of the required 145 bars. Some time previously, the manufacturer had carried out an operation on these sensors to limit chatter on the pressurizer water spray valves. This operation, which should not have had any effect on the sensor settings, in fact caused their zero setting to shift. The anomaly was corrected by cross-calibration between these sensors and the reactor coolant system pressure sensor located at the RHRS intake, using a deadweight pressure tester. This event did not result from the use of a measuring or adjustment instrument, but is similar to the Chooz A event with regard to the observed facts.
- In July 1988, a human error in maintenance resulting in an incorrect pressure setting on a steam generator mechanical safety relief valve at Unit 3 of the Paluel nuclear power plant caused the valve to open at 76.2 bars. This event, although it does not necessarily have the same origins, is similar in its consequences to the event that affected Tricastin nuclear power plant Unit 2 in April 1989.
- Faulty operation of a recorder used when checking the settings of the same steam generator safety relief valves at Unit 2 of the Fessenheim nuclear power plant in March 1990 was at the origin of a setting error in the assist units, causing several safety relief valves to open.
- In September 1991, during the restart physical tests at Unit 2 of the Chinon B nuclear power plant, a difference was observed between the theoretical critical boron concentrations with all RCCAs withdrawn and bank R inserted, defined by the EDF Nuclear Computing Division, and the values measured on site in the same conditions using the analyzer. This difference was due to an error in the concentration of the sodium hydroxide used to measure the boron concentration in the facilities, resulting in all the measurements made in units 1 and 2 being underestimated by 5.5%. In response, the facility operator adjusted the boron concentrations in the tanks and reset the automatic boron meters that measure the reactor coolant system boron concentration in the two reactors. After the error was corrected, the boron concentration in some of the borated water tanks was found to exceed the upper limit of the technical specification.

Analysis of the events due to measuring or calibration equipment identified three main causes: use of a faulty instrument, use of an inappropriate instrument and improper use of an instrument. It showed the need to raise the awareness of the personnel involved regarding the common-mode character of such faults, which can affect more than one equipment item.

The lessons learned led EDF to produce an internal directive, *Étalonnage et vérification des appareils de mesure et des étalons* (Calibration and Verification of Measuring Instruments and Standards), and all sites have been required to comply with this directive. The directive reproduces the main points of a policy document entitled *Doctrine d'étalonnage et de vérification des appareils de mesure et des étalons* (Calibration and Verification Policy for Measuring Instruments and Standards), which covers the calibration and verification actions to be implemented in order to limit risks related to use of faulty measuring or calibration instruments, in particular the risk of common-mode failure when working on redundant components. These measures fall within the more general framework of prevention of common-mode events (covered by the document *Prévention des défaillances de mode commun* [Prevention of Common-Mode Failures]).

In view of these events, the safety organizations considered that a questioning attitude had to be encouraged among the personnel involved in such work. In particular, it was important to restate and circulate the following fundamental rule: when a given correction must be made systematically on two or more components, there is a significant risk of common-mode errors or faults due to the use of a measuring or calibration instrument, and a specific analysis must be undertaken. This rule is intended to avoid a large number of events. Its application would have enabled early detection of most of the anomalies discussed above. Recommendations have been formulated to supplement the EDF directive and to improve its implementation. Lastly, the principles that aim to prevent risks related to work on redundant trains were restated: where possible, schedule work of the same type on redundant components at different times; conduct functional requalification of the components after the work.

22.2.2. General discussion initiated by EDF in the late 1980s on the quality of maintenance operations

Only a few major points of EDF's analysis are discussed here:

- **Common-mode failure risks:** maintenance operations on redundant components can lead to the same anomaly on all the trains, in particular when operations are scheduled together in the same time period. This may consequently result in total loss of the protection system or engineered safety function concerned. EDF attempted to identify all such operations, but this task appeared difficult, since it is necessary to take into account the potential common mode to ensure safety, knowing that these operations may involve not only scheduled operations, but also unscheduled operations. These risks must therefore be kept in mind constantly by the people responsible for managing outages and the work performed. Analyses showed that operations planned in the basic maintenance programmes for which the period given is longer than one year should be scheduled over several outages.

- **Management of Temporary Measures and Devices**[655]**:** several events caused by forgetting to recover temporary parts used for a test or other work have occurred in French nuclear power reactors. Temporary measures and devices are many and varied. Some are planned in the design stage, for example the blind flanges at the bottom of the reactor pool and the reactor vessel internals compartment, which must be installed in order to be able to fill these pools during fuel handling operations. They must be removed before the reactor is set into operation in order to avoid spray water retention in these pools in the event of an accident requiring containment spray system operation. The removed blind flanges are placed in dedicated racks; an alarm window in the control room is lit if any of the flanges are not in the appropriate rack. Their management does not raise any particular problems. The same management and tracking methods are not applied to most of the other temporary mechanical devices (plugs, filters, etc.). These are normally stored in cabinets with transparent doors and can be monitored by visually checking the cabinet contents.
- The electrical temporary measures and devices used most often are temporary connections (jumpers) and terminal boxes. Jumpers are normally identified in place by a different colour from the normal wiring and a label. They are managed administratively in the 'jumper log' available in the control room. The jumper management procedures were reviewed in the context of experience feedback from the Chernobyl accident, with regard to the risk of engineered safety system inhibition. The location of small terminal boxes can only be checked by opening the cabinets housing them. A number of incidents have shown that this method was not completely effective.
- Several hundred temporary measures and devices are used during an outage. Overall, a large proportion of temporary measures and devices are managed using various documents, various IT resources or physical management

[655] Subsequently, temporary modifications to installations, covered by the 'Procedures' decree, were included in the approach. A Temporary Measure or Device corresponds to a precise definition given by the facility operator in a corporate directive:
- a Measure is the result of an action taken to modify the position or setting of an equipment item in the facility;
- a Device is, for example, an actuator, valve, part or component installed on or removed from a system or a portion of a system;
- measures or devices are temporary when their use modifies the functional state of the facility temporarily and when their use, other than in the reactor unit or system states for which they were initially intended, introduces a risk for safety, availability or security;
- a Temporary Measure or Device must only be used if an initial analysis has shown that it is necessary. Its use must be temporary. Any use of a Temporary Measure or Device is subject to:
  - prior analysis of the need and any related risks,
  - administrative management to ensure its traceability and local indication of its presence throughout the time it is used,
  - measures to ensure that it has been removed, giving preference to functional tests or, when that is not possible, local checks.

(the pool bottom blind flanges, for example). This is not necessarily the case for states configured or devices used for short durations, by a team carrying out the entire operation, from implementation/installation to restoration/removal. As the compilation of an exhaustive list was unrealistic, EDF sought to decentralize their management close to the teams using them, while issuing a specific directive at corporate level (DI 74).

– **Equipment requalification after work:** the principle of requalification after work is applied by EDF only if the conditions of the operation and the management procedures for temporary measures and devices do not provide adequate guarantees. It is then necessary to define in each case what must be requalified, using which procedure and when. In practice there are two categories of test documents available for conducting requalification during reactor outages:

    - the Startup Test Operation Sheets, which are in principle complete and can be used for both qualitative and quantitative verification of all the functions; however, their implementation may require a reactor state not planned during the outage. Furthermore, once a reactor has been started up, operating personnel no longer has ongoing practical experience or even adequate knowledge of the startup test operation sheets;
    - the Periodic Test Operation Sheets, which can be used to check that the performance of systems on which no work has been done is maintained over time; they can be used directly, but may not be sufficient. They must be used in an appropriate reactor configuration.

  Although the safety organizations agreed that whether requalification tests were necessary after work on equipment depended on a case-by-case analysis, they strongly encouraged EDF to give preference to such tests as much as possible.

– **Safety Quality Approach:** discussions conducted by EDF led it to produce a framework for discussion enabling better organization of the various operations, keeping in mind defence in depth (for example by postulating unforeseen events in the execution of operations in order to determine how to recover from them or mitigate them). This preparation approach includes conducting a risk analysis based on a risk analysis guide. The guide covers several dozen potential faults, illustrated by examples, including common-mode failures, confusion in identifying equipment, generation of unavailability, forgetting configurations implemented and test equipment installed temporarily, inadequate cleanness, and hazards due to nearby equipment. In applying this approach, orders of priority are assigned to preparation, execution, inspection and requalification work. It may also lead, if possible, to not work on the different trains of a redundant system during the same outage (the idea of having such work performed by different teams was not pursued, as it would multiply the number of personnel involved). If analysis identifies a particular risk, work preparation includes preparation of a Safety Quality Plan that explains how to prevent risks, the necessary hold points and corresponding checks, how to cope with any incidents during the work, and the needs and methods for requalification. The Safety Quality Plan is used to track the operation itself and to record the results of the various checks and any anomalies encountered. This practice, completely favourable with regard to safety, was implemented gradually, with priority given to work on engineered safety systems.

The analysis conducted by EDF led to other changes[656], including:

- providing training facilities for preparing complex operations,
- making reactor unit outage project structures permanent (see Section 25.4), and making project and oversight managers permanent for managing work and operations conducted during unit outages,
- redefining the scope of activities assigned to the operations shift managers, and scheduling the safety engineers 'off-shift' to ensure genuine independence in their supervisory activities,
- extending safety engineer involvement in maintenance activities,
- reinforcing the Safety Quality Team[657].

22.2.3. Applying the defence-in-depth concept when working on a reactor in service

Although the defence-in-depth concept is first and foremost applied in support of the facility design approach, its principles can also be applied to work that a facility operator must carry out on facility equipment while it is operating, whether it involves periodic tests, maintenance operations or changes.

For this purpose, the concept can be divided into three main stages:

- prevention of events and anomalies occurring during the work, or later, as a consequence of the work, which can be achieved by:
    - careful preparation of the operations and associated documents,

[656] See Chapter I, Section 4.3.2.2 of *Mémento sûreté nucléaire en exploitation* (Memento on Operational Nuclear Safety), EDF, 2016 edition.

[657] Subsequently the Safety Quality & Environment Team: this unit is part of the Corporate Technical Support Department (UTO) of the Nuclear Power Generation Division (DPN) at EDF. UTO is the national entity responsible for nuclear power reactor maintenance engineering. Its mission covers equipment repair and procurement of spare parts and components managed at corporate level, representing the project owner for maintenance operations conducted at nuclear facilities, producing technical specifications for corporate level procurement and service contracts, and selection of referenced service providers and contractors. Within UTO, the Safety Quality & Environment Team has a staff of about ten people responsible for independent assessment of the trades and professions working in operations, with a focus on safety and environmental protection.

   - availability of clear worksheets consistent with the state of the facility,
   - evaluation of the potential risks,
   - verification of the compatibility of the planned actions with the state of the facility, given the downtime rules defined by the operational limits and conditions,
   - preparation of tools used for traceability and monitoring purposes,
   - identification of potential mitigation devices and systems,
   - assignment of a sufficient number of qualified personnel,
   - strict application of the prepared documents,
   - the requalification process required by the work;
- – overseeing the work, ensured by:
   - periodically checking work in progress, tests, visual inspections, field inspections, hold points,
   - comparison of the results obtained with the required results and detection of anomalies,
   - sharing information when anything unexpected is observed;
- – mitigation of events or anomalies by:
   - advanced definition of planned fallback states,
   - use of automatic or manual equipment or systems, which must also be defined in advance.

22.2.4. Problems that may recur

Some of the issues raised by the analysis of the events reported above may recur, which highlights the need for facility operators and operations personnel to continuously keep a watch on the quality of work conducted on the reactors.

In particular, an event that occurred in January 1999 at Unit 1 of the Nogent-sur-Seine nuclear power plant emphasized the importance of the risks of common-mode failures associated with electrical settings. Similarly, an event that occurred in April 2005 at Unit 3 of the Gravelines nuclear power plant once again highlighted the risks related to temporary measures and devices.

These two events are discussed in Chapter 23.

Chapter 23

Operating Experience from Events Related to Maintenance Operations, Electrical Power Sources and Distribution, Internal and External Hazards

A number of significant events that occurred since about the mid-1990s are examined in chapters 23 and 24. Some of these events shed light again on past events, such as those that led Électricité de France (EDF) to take measures to improve the quality of maintenance operations (see Chapter 22).

Discussion in this chapter is limited to events related to maintenance operations, electrical power sources and distribution, and internal and external hazards. The partial flooding of the Blayais nuclear power plant site, concomitant with the storm that occurred in France in late December 1999, and the event at the Cruas-Meysse nuclear power plant in early December 2009 caused by seaweed in the site water intakes, two events that deserve special attention, are described separately in Chapter 24.

23.1. Risks of failure related to equipment or maintenance

23.1.1. Risks of common-mode failure

23.1.1.1. Risks of common-mode failure related to settings

(Nogent Unit 1 – January 1999)

In the late 1990s, an event occurred that recalled the importance of risks due to common-mode failures caused by incorrect electrical settings. The event occurred in January 1999 at Unit 1 of the Nogent-sur-Seine nuclear power plant during an islanding test: it resulted in loss of an electrical power train of the essential service water system (ESWS) pumps and the reactor coolant system makeup water transfer pump.

The islanding test consists of checking the ability of a nuclear power reactor to disconnect itself from the electricity grid while switching over to autonomous operation at reduced power. With the reactor at its nominal power, the test is initiated by opening the main off-site power line circuit breaker. The opening of the circuit breaker resulted in loss of electrical power train A of the essential service water system (ESWS) pumps and of the reactor coolant system makeup water transfer pump (charging pump). The pump motors were tripped because of incorrect setting of the activation thresholds of their power supply current overload protection relays. The thresholds had been set when maintenance was carried out on the train A electrical switchboards during a refuelling outage. Investigations by the facility operator after the event showed that the current thresholds had been set to values 6% to 30% below the value specified for all equipment supplied with 6.6 kV by the emergency-supplied switchboard (11 actuators concerned, including those of all engineered safety system pumps) and for the equipment supplied by the non-emergency-supplied switchboards (23 actuators). The incorrect setting of the thresholds was detected during the islanding test by the high (but normal for this transient) frequency of the electrical power supply in the stabilization phase of the reactor at reduced power after islanding. The frequency acts directly on the pump rotation speed and therefore on the pump power input and the current drawn by the motors. In the case discussed here, the frequency was close to 52 Hz, resulting in a current higher than the current at the nominal frequency of 50 Hz. The higher current draw, combined with the incorrect low setting of the protection thresholds, caused the motors to trip.

Shutdown of the ESWS pumps and of the train A charging pump caused automatic startup of the equivalent pumps supplied by electrical train B. As the train B protection threshold settings were correct, train switching proceeded normally, within 15 s for the charging pump and within 55 s for the ESWS pumps. These short interruptions, taken into account in the design, did not degrade the state of the reactor. Moreover, continuous cooling of the reactor coolant pump thermal barriers by a train A component cooling water system (CCWS) pump (its protection threshold setting incorrect but not low enough for it to trip) during the interruption of injection at seal 1 averted damage to the seals. In conclusion, this event did not have any real consequences, because the train B electrical protection thresholds were set correctly. In this case, it appears that application of the prevention principle of staggering the scheduling of maintenance operations of the same type on redundant trains avoided an H1 situation (total loss of heat sinks).

Based on EDF's analysis, it appears that the underlying causes of the event were located at several levels:

- incorrect application of the checking and setting work sheet used by maintenance personnel to set the electrical protection thresholds. It should be emphasized that the operation was carried out by two people who, although experienced and qualified, had never performed this operation before;
- lack of a questioning attitude of the personnel involved on the consequences of complete resetting of the switchboard protection thresholds. The threshold values recorded by the personnel in the first check were within tolerance but close to the upper limit. It was the decision of the personnel to reset the settings to values in the middle of the tolerance interval that led to the incorrect settings. This attitude pointed to shortcomings in operator training on this type of setting;
- a single maintenance work sheet for checks and settings. Furthermore, the work sheet was common to three different types of printed-circuit board, which required different settings, but did not specifically warn personnel that there were critical phases requiring special attention;
- lack of traceability of the actions performed during the operation, meaning that the actions could not be checked. Only the value of the current threshold after setting was recorded in the work sheet report; this value had to be within the tolerance interval of the required value. Any setting renewals were not mentioned, significantly reducing the possibility of detecting anomalies or incorrect actions when the 'completed' work sheet was checked;
- inadequate intrinsic and functional requalification steps for detecting this type of anomaly.

The safety organizations restated the importance of the electrical protection settings, which show a degree of analogy with the settings of the core measurement and protection systems, classified as 'sensitive parameters' by EDF. An analysis was then conducted covering all the nuclear power reactors with a view to defining measures for reducing the risks of setting errors.

23.1.1.2. Risks of common-mode failure on electrical switchboards

(Cruas Unit 4 – October 1990)

In October 1990, initiation of arcing on a pole of the contactor supplying an ESWS pump at Unit 4 of the Cruas-Meysse nuclear power plant caused a local explosion, fire and destruction of the main emergency-supplied switchboard of train B

(LHB), rendering all the engineered safety features of the train unavailable. Ageing of shock-absorber rings inside the contactor was the underlying cause of this event.

The situation was managed without release or threatened release of radioactive substances.

The event nevertheless provided evidence of potential common-mode failures that could affect the two emergency-supplied main switchboards LHA and LHB, by ageing of identical rings in both switchboards. This ageing had been identified, but corrective measures were still being defined.

The event also showed that a fault affecting a component located downstream of an electrical switchboard could cause the switchboard to fail; this had not been included in the safety studies, as the protection against electrical faults was considered highly effective. However, an event had previously occurred in June 1986 at Unit 2 of the Paluel nuclear power plant, during which the incorrect position of an earthing disconnecting switch led to connection of the gas turbine. The lack of an operating procedure covering the situation of loss of emergency-supplied switchboards with the upstream switchboards powered had been noted then. The Cruas event led to the introduction of an appropriate procedure.

The rings were rapidly replaced in the electrical switchboards fitted with them. Several reactors were involved.

23.1.1.3. Unavailability of two out of three high-head safety injection lines in the cold legs of the reactor coolant system

(Blayais Unit 3 – August 2008)

On 9 August 2008, while Blayais nuclear power plant Unit 3 was being shut down for refuelling, a boric acid solution at 21,000 ppm boron was injected into the reactor coolant system in application of the periodic testing programme. This injection, planned at each refuelling outage, is performed to check availability of the safety injection function.

The facility operator measured a water injection flow rate of 60 m^3/h instead of the expected 100 m^3/h. Investigations on the components likely to reduce the flow rate showed that crystallized boron was present in two out of the three valves on the safety injection lines in the reactor coolant system cold legs (‘A’ valves in Figure 23.1). Partial obstruction of these lines by the crystallized boron explained the low flow rate observed. The origin of this problem in fact dated back to March 2008; it was linked to the repair of a motor-driven valve located immediately upstream of the tank containing boric acid at 21,000 ppm boron (‘B’ valve). For the needs of the repair, this valve was kept open for longer than an hour. Consequently, during this period, the boric acid tank and the portion of the adjoining system as far as the downstream isolating valves (‘C’ valves) had been exposed to the pressure exerted by the high-head safety injection pumps, about 170 bars. Because of the accepted leakage rate for these valves, there was a pressure increase in the lines located downstream, in the system portions located between the C valves

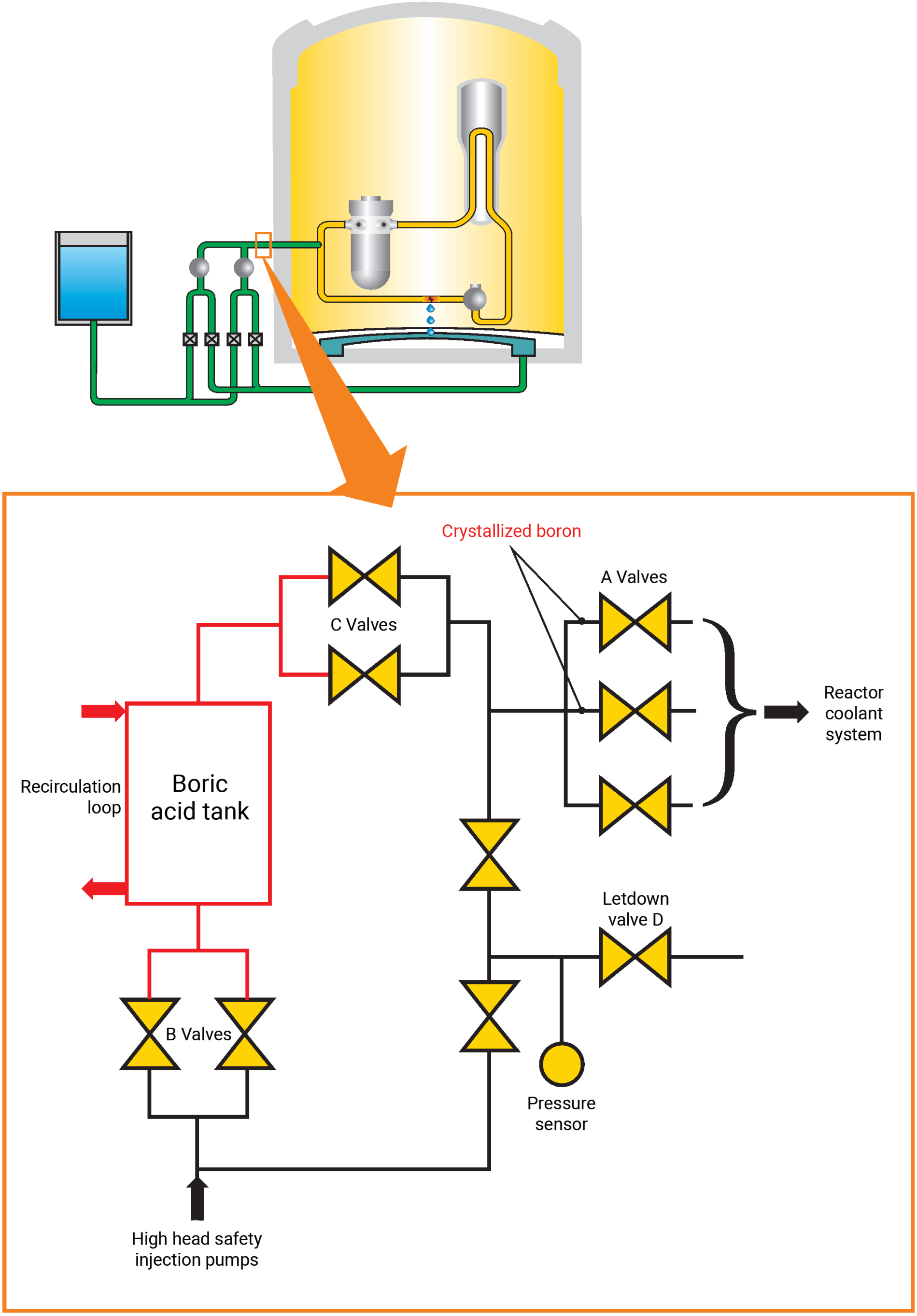


Figure 23.1. Simplified diagram of the system involved in the August 2008 event at Unit 3 of the Blayais nuclear power plant. Georges Goué/IRSN.

and the cold leg isolating valves (A valves). The system pressure was monitored to detect any leakage and, if necessary, the pressure could be reduced by opening a letdown valve ('D' valve) provided for this purpose. The facility operator therefore opened the D valve to depressurize the line; however, the operating procedure stated that this valve should only be opened for a short period, limited to the time strictly necessary for depressurization. By keeping the D valve open for an hour, the facility operator did not comply with the instruction, thereby favouring the transfer of boric acid at 21,000 ppm boron into the portion of the system between the C valves and the A valves. The A valves do not have any means of maintaining a temperature that would avoid crystallization of boron at such a concentration, so boron crystals formed and accumulated, given that the flow cross-section of the A valves is significantly smaller than that of the rest of the system. The obstruction of one of the three valves was cleared under the effect of the pressure, resulting in an established flow rate of 60 m^3/h; the other two valves remained obstructed. To return the facility to a compliant state, the facility operator proceeded to clean the valves to remove any trace of boron, and conducted a full test of the safety injection system. This test confirmed that the system was again operational.

In the case of a loss-of-coolant accident, the obstruction of two out of three safety injection lines by crystallized boron would have resulted in a lower injection flow rate than specified. Consequently, fuel cooling would have been less effective and perhaps even insufficient. Moreover, the amount of boric acid at 21,000 ppm boron would have been injected into the reactor coolant system over a longer period, and thus would have been less effective in providing negative reactivity.

Boron crystallization had already been observed in 900 MWe reactors. Its origin, its frequency in different parts of system lines and its consequences for safety (which may be significant) were analysed. Based on the results, EDF had defined measures to be taken at facilities with regard to each identified risk. The measures were based mainly on operating instructions (system monitoring, checking for obstructions, pipe flushing as necessary, etc.). It appears that the event at the Blayais nuclear power plant, which resulted from non-compliance with an operating instruction, was also a consequence of lack of perception of the crystallization risk by the operators, which showed the limits of the recommendations.

It also demonstrated that the occurrence of unforeseen events under normal facility operating conditions could have major consequences on facility safety. It is therefore essential to carry out an appropriate analysis of all the risks that might result from such events so that appropriate countermeasures can be taken. Moreover, the event was also a reminder that a questioning attitude is essential for detecting anomalies (safety culture). It also showed that, despite the inspections and periodic tests to ensure the availability of the engineered safety systems, some latent faults can escape detection by operators.

After the event, EDF introduced new measures: stricter operating instructions, accompanied by actions raising operator awareness of the boron crystallization risk, and a new stricter criterion for permissible leakage of the valves downstream of the 21,000 ppm boric acid tank.

23.1.1.4. Loss of electrical power supplies

▶ Gradual loss of three out of four electrical power supplies

(Bugey Unit 5 – April 1984)

In April 1984, at Unit 5 of the Bugey nuclear power plant, the voltage of an instrumentation & control DC supply started to decrease slowly following a fuse failure on the battery power supply unit. The battery power supply alarm, grouped with other frequently triggered alarms[658], was not identified by the control room operators. The low instrumentation & control (I&C) supply voltage caused the reactor trip breakers to open, resulting in an RCCA drop and reactor shutdown.

Switch-over of the electrical power supplies, controlled by the same insufficient power supply voltage, was not completed correctly. The reactor was no longer supplied by the power transmission line nor by the auxiliary power line.

The diesel generators received the startup command. The AC generator of the faulty train did not have an excitation voltage, so it could not supply electrical current. The other diesel generator started up normally and provided the emergency supplies to the necessary equipment of the corresponding train. This equipment is designed to be sufficient to ensure the safety of the reactor in the shutdown state.

Poor operation of the pressurizer letdown and relief valves, due to loss of their electrical power supply, led to a significant pressure increase in the reactor coolant system. Other faults resulting from the initial failure interfered with transmission of certain items of information to the control room; some of them were false, but plausible.

This was consequently a situation of loss of three out of four electrical power supplies, an obvious precursor to a total loss of electrical power supplies, which affected a reactor unit that did not yet have the necessary equipment or procedure to cope with it, and was furthermore disturbed by instrumentation & control electrical power supply failures.

The operators had not been prepared for this situation and they did not have appropriate operation documents. The know-how of the team nevertheless allowed the situation to be managed correctly.

The case of a slow voltage decrease on the DC switchboards had not been considered in design studies, which only covered cases of outright failure of the electrical power supplies.

The equipment necessary to cope with a total loss of electrical power supplies, still under study at the time, has since been installed on all French reactors.

[658] These alarms report electrical insulation faults on a set of cables used during the construction of the reactor unit. The faults were known, their consequences minor. No operator action was required, pending replacement of the cables in question.

The event also led EDF to accelerate studies and work on upgrading the alarms, and to develop protection against slow decreases in direct current voltages and, more generally, against failures of low-voltage electrical supplies.

Lastly, the first state-oriented approach procedures, in particular procedure U1 (see Chapter 33) associated with a procedure for monitoring the state of the instrumentation & control electrical supplies, have enabled complex situations to be dealt with, without improvisation.

In March 1987, at Unit 1 of the Gravelines nuclear power plant, a voltage decrease on an alternating current (AC) switchboard supplying the reactor protection system caused disturbances leading to a deviation outside the authorized operating domain. This event led EDF to initiate discussions and undertake actions similar to those implemented in the case of the Bugey Unit 5 event, this time for voltage decreases on the AC switchboards.

▶ Reactor fallback due to unavailability of a 6.6 kV LHA electrical switchboard – Tin whiskers formation[659]

(Dampierre-en-Burly nuclear power plant – April 2007)

On 9 April 2007, Unit 3 of the Dampierre-en-Burly nuclear power plant lost the electrical power supply to train A safety equipment. The event was caused by failure of an overcurrent protection relay on the LHA electrical switchboard. The failure made it impossible to connect the emergency generator to the LHA electrical switchboard; the train B safety equipment could still be supplied by the LHB electrical switchboard. In compliance with the procedures applicable to this type of fault, the facility operator initiated a reduction of the reactor power (initially at 60% of its nominal power) with a view to shutting it down.

During the reactor shutdown procedure, when the turbine tripped, another fault, on the main off-site power line (in the generator breaker connecting the turbine generator to the grid), made the situation worse (the line breaker had opened), resulting in loss of the electrical power supply to the nuclear power plant by the main off-site supply line.

In this situation, the auxiliary off-site power line normally takes over from the main line automatically. During the event on 9 April, this switch-over did not take place. The total loss of off-site power led to reactor trip and automatic startup of the train B emergency generator. The reactor was brought to the shutdown state defined for such a situation using the train B safety equipment. Subsequently, the secondary cooling system continued to cool the reactor by circulating reactor coolant system water in thermosiphon mode (natural convection). However, on the morning of 10 April, before the planned shutdown state was reached, the auxiliary off-site power line and safety electrical train A were recovered, making it possible to start up a reactor coolant pump and resume forced circulation of water in the reactor coolant system.

[659] Tin burr or filaments.

Had the train B emergency generator failed, the reactor would have been in a Station Blackout (SBO) situation. This situation would have had to be managed by procedure H3, which relies on an emergency turbine generator to power the minimum resources for controlling the facility. An EFWS turbine-driven auxiliary feedwater pump was also available to supply water to the steam generators and thus cool the reactor. French nuclear power plants also have a station blackout diesel generator (one per site). The preliminary operations for connection of this generator to the train B electrical switchboard had been completed in order to compensate for any failure of the train B generator.

Several failures were identified during analysis of the event.

The first concerned an overcurrent protection relay, which had caused the loss of electrical switchboard LHA. An identical hardware failure had already caused an event concerning Dampierre-en-Burly nuclear power plant Unit 1 on 16 November 2000. After that event, the facility operator had introduced measures to monitor these relays and procured a new generation of protection relays to replace them. The new relays were available at the Dampierre-en-Burly nuclear power plant but had not yet been installed.

Subsequent assessment of the failed relays showed that the event was caused by the formation of zinc filaments similar to tin whiskers. The filaments had formed conductive bridges between the conductors of the printed circuit board or the electronic components and the zinc dichromate plated sheet shielding of the electronics. These bridges can cause insulation faults or trip a relay.

Investigation by the facility operator showed that nearly all the protection relays were affected by the formation of metal filaments in variable amounts and sizes.

As stated above, during the reactor unit shutdown required by the procedures, a second fault was detected on the generator breaker, located at the turbine generator output, which trips the turbine when power is below 10%. The generator breaker took an abnormally long time to open, resulting in automatic disconnection of Unit 3 from the main off-site power line by opening the line breaker located downstream of the transformer. The fault could not be reproduced during subsequent testing. Subsequent assessments were also not able to determine the cause of the anomaly.

Furthermore, during the event, automatic switch-over to the auxiliary power line did not take place, as its instrumentation & control circuit had been deliberately cut off at the start of the event, in compliance with operating procedures. These measures, concerning the I&C switchboards of equipment not considered essential, were intended to reduce emergency battery consumption and thereby limit the risk of transmission of spurious commands.

EDF was aware of the tin whiskers formation observed in other countries, but had never observed it itself, because it replaced printed circuit boards as soon as they caused operating anomalies. The event revealed that tin whisker formation also affected electronic components at French facilities, leading to equipment changes intended to eliminate the formation of these metal filaments.

EDF decided to deal with the tin whiskers problem by replacing the shielding sheets of the existing relays, after repair by the manufacturer, or by installing new relays of a more recent generation. With regard to the automatic control of switch-over to the auxiliary electrical power supply in the case of loss of the LHA switchboard until turbine trip, the facility operator introduced a measure that avoids short-term isolation of the battery supplying the I&C switchboard of the control device that switches the reactor electrical power supply from the main supply to the auxiliary supply, thereby limiting the risk of total loss.

23.1.2. Introduction of non-borated water into the reactor coolant system

▶ Introduction of non-borated water from the secondary cooling system

(Blayais Unit 4 – March 1990)

In March 1990, at the end of a refuelling outage at Unit 4 of the Blayais nuclear power plant, when the reactor coolant system water level was located approximately at the median plane of the system loops, an inadvertent boron dilution was caused by leakage of non-borated water from the secondary side of a steam generator.

Errors in lockout measures resulted in the secondary side of the steam generators being filled too soon, causing non-borated water to spill into the channel head of a steam generator, since a tube on this steam generator, cut off on the hot leg side, had not yet been blanked off on the cold leg side (see Figure 23.2). Observation of water flowing through the channel head manway on the cold leg side led to installation of an inflatable plug in the manway, following an instruction intended to cope with potential water leakage from the reactor coolant system at a nozzle dam. In fact, the channel head on the cold leg side filled up and was pressurized under the effect of the secondary cooling system water column. The nozzle dam in place between this channel head and the reactor coolant system cold leg, under pressure in the direction contrary to what it had been designed for, gradually lost its leaktightness. The introduction of non-borated water only stopped when the steam generator was drained.

However, action taken by the operators kept the boron concentration in the reactor coolant system water above the minimum value specified in the operational limits and conditions. The flow rate of non-borated water introduced into the reactor core remained compatible with the assumptions made in the situations examined in the safety analysis reports. The event nevertheless showed a potential accumulation of non-borated water from the secondary cooling system in a loop of the reactor coolant system.

A more sudden failure of the installed nozzle dam could have caused rapid flow of a major part of the 4 m^3 of water contained in the cold leg channel head to the reactor core, generating a larger transient.

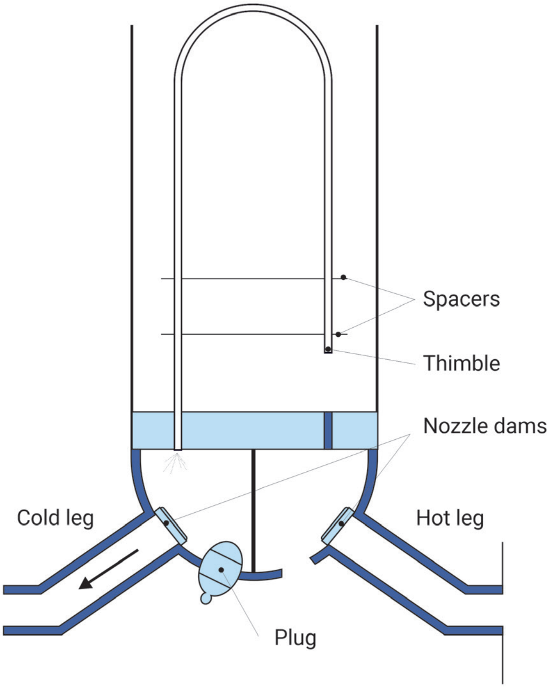


Figure 23.2. Diagram of the steam generator, the cut-off tube and the channel heads. Georges Goué/ IRSN.

Moreover, had the anomaly occurred when the cold leg channel head was already closed (with the nozzle dam removed), its identification would have been much more difficult. During reactor coolant system venting, starting the pump of the loop concerned could have caused rapid flow of the non-borated water contained in the cold and crossover legs into the core. The water in this loop was not kept moving by the residual heat removal system. The consequences on the core would have approached the conditions for fast criticality; knowledge of these conditions by the operators contributed to their successful management of the situation.

▶ Introduction of non-borated water from an accumulator

(Belleville Unit 2 – July 1990)

The event occurred after the hydrotest of an SIS accumulator at Unit 2 of the Belleville-sur-Loire nuclear power plant in July 1990, when the facility operator was testing the operation of the accumulator's isolating valve. The reactor vessel was open and filled with water up to the plane of the closure head seal. Core cooling was being provided by the residual heat removal system.

During the hydrotest, conducted one month earlier, the accumulator had been filled with non-borated demineralized water. All of this water should have been drained after the hydrotest and before the valve opening test. In fact 16 m^3 of water remained in the accumulator; this could not be detected by the water level measuring device in the accumulator, which only covered a narrow range.

The opening of the isolating valve allowed non-borated water to flow by gravity into the reactor coolant system. The flow rate of the residual heat removal system circulation ensured immediate mixing of the non-borated water with the borated water in the system. Although the boron concentration consequently fell below the value stipulated by operational limits and conditions, it nevertheless remained sufficient to keep the core from returning to the critical state. The operator was alerted by reactor coolant overflowing at the level of the closure head seal, and closed the valve.

The accumulator vent should have been open during the test. The fact that it stayed closed slowed and limited the water transfer. With the vent open, the isolating valve kept open and a lower flow rate in the residual heat removal system, the result could have been a more rapid introduction of less-well-mixed water and consequently a risk of critical power excursion.

This was an example of a situation that was a precursor to sending non-borated water into the reactor core as a consequence of maintenance operations.

Following this event, the facility operator decided that the hydrotests on tanks and vessels connected to the reactor coolant system would use borated water at the same concentration as the reactor coolant system in cold shutdown.

23.1.3. Cooling the reactor coolant system after inhibition of automatic actions

(Paluel Unit 2 – January 1993)

In January 1993, Paluel nuclear power plant Unit 2 was in the restart phase after refuelling. The normal procedure included testing automatic startup of the steam generator emergency feedwater system (EFWS), activated in the event of failure of the normal feedwater system (MFWS). This test had to be performed at a reactor power compatible with the EFWS heat extraction capacity (2% of nominal power).

The test was undertaken by mistake when the reactor power was three times higher. However, the error was detected rapidly. The shift crew inserted the RCCAs until reactor shutdown, without causing reactor trip, and proceeded with borated water makeup to obtain the boron concentration required for the core in a shutdown state.

During the test, a condenser steam dump valve remained partly open, even though it had received a command for complete closure. This partial opening caused substantial cooling of the reactor coolant system, at 70°C/h instead of the 56°C/h permitted by the operational limits and conditions in an incident situation (the limit in normal condition is 28°C/h).

Two items of information related to the position of the valve were available in the control room:

– position information indicating that the valve was ‘not closed’; however, this information was considered as perhaps unreliable;

– control system information indicating ‘100% closed’.

The operators observed that the reactor coolant system was cooling at an excessively fast rate, but interpreted it as resulting from the low residual heat of the reactor in the restart phase and an excessive steam generator emergency feedwater system flow rate. To avoid yet faster cooling, the operators requested authorization from the shift manager to inhibit the safety injection for ‘cold leg very low temperature’. This protection action is intended to cope with inadvertent opening of a steam relief valve (which was in fact the actual situation). It activates the safety injection system and the steam generator emergency feedwater system at full flow (which would have further accelerated the cooling), but it also closes the main steam line isolation valves, which would have terminated the event by isolating the secondary cooling system upstream of the leak.

The shift manager, occupied elsewhere, authorized the action, knowing that the boron concentration in the reactor coolant system water was close to the concentration required when cold. He also requested a search for the causes of steam consumption by the system.

As the rapid cooling continued, the shift crew inhibited a second command to activate the safety injection, for ‘pressurizer low-low pressure’. It used a procedure valid in normal operation, but not during an incident transient.

The failure of the steam dump valve to close was not detected until 50 min had elapsed; the valve was closed 30 min later.

At no time was the safety engineer on the site called to the control room, because the signals for which the engineer is formally required to be called (such as reactor trip) were not triggered.

The initial event (condenser steam dump valve closing failure) is covered by the studies described in the safety analysis reports. The potential consequences are core return to criticality accompanied by reactor cooling system water boiling near the fuel assembly containing the most reactive RCCA, assumed in the studies to be jammed in the raised position.

The actual situation was less unfavourable than the situation considered in the safety studies, as the steam dump flow rate through the valve and residual heat were both lower. Moreover, at cycle start, the moderator temperature coefficient of reactivity is much lower than at cycle end. The risk of fuel damage was consequently low.

The importance of this event lies above all in the fact that safety measures were inhibited when they should not have been and that, more generally, there was an incorrect real-time analysis of the situation, with lack of redundancy of the diagnosis between the shift crew, the shift manager and the safety engineer.

Its late declaration only confirmed these deficiencies.

Independently of the repair of the faulty valve, the corrective measures in this case concerned more particularly the organization of the facility, its working methods and the allocation of responsibility.

23.1.4. A temporary device prevents switching the safety injection system to the water recirculation mode

(Gravelines Unit 5 – April 2005)

Chapter 22 describes several events that occurred in 1989 and 1990 related to temporary measures and devices[660]. In the 2000s, the event described below pointed again to the risks related to temporary measures and devices.

During the refuelling outage of Gravelines nuclear power plant Unit 3 in April 2005, the facility operator carried out a periodic test of safety injection, with the reactor vessel open and unloaded, in accordance with the timing conditions defined by the periodic test programme. The reactor trip breakers must be closed for this test[661]. These breakers were in fact open and not operable. In order to work around this contingency and comply with the outage schedule, the facility operator implemented a temporary measure by disconnecting two electrical wires in the instrumentation & control of the reactor protection system (one on train A and the other on train B) to simulate the closed position of the breakers.

The wording of the work order for the temporary measure was not sufficiently precise and left the technician the option of disconnecting the wires at two different locations. On completion of the work, the person responsible for restoring a compliant state did not have the same interpretation as the technician who had disconnected the wires. The person went to the location where the wires had not been disconnected, and concluded that they had already been reconnected, without making any other checks.

Similarly, when the relays of the reactor protection system were checked at the end of the outage, no-one noticed that the wires were disconnected. It was only at the beginning of the next outage (i.e. one year later) that the check on the protection system relays detected the two disconnected wires. Analysis of the event showed that neither the two-monthly tests nor the functional tests performed at each refuelling outage were able to detect this anomaly.

When the reactor trip breakers are opened after a reactor unit protection command, a signal is generated to enable a reset of the safety injection signal stored in memory. The disconnection of the two cables in the reactor protection system disabled the option of resetting the safety injection command by the operators on the two redun-

[660] This concept is discussed in detail in Section 22.2.2.

[661] The breakers open when a command is sent to activate reactor protection.

dant trains of the system. In the event of a major loss-of-coolant accident, this anomaly would have prevented automatic switching of the two safety injection system trains to water recirculation through the containment sumps. If the facility operator had not taken action, the safety injection system tank would have been drained completely, and the pumps would then have run dry, resulting in their destruction, consequently interrupting cooling and leading to fuel uncovery in the core.

Similarly, if a steam generator tube rupture accident occurs, a reset allows safety injection to be stopped from the control room in order to limit release to the atmosphere. It would also have been impossible to operate the valves and shut down the motor-driven pumps on the steam generator emergency feedwater system from the control room.

Following this event, EDF introduced an action plan to further enhance reliability of the processes used to manage temporary measures and devices and to reinforce periodic checks on the reactor protection system.

In this context, operating experience feedback had already shown that an engineered safety function could be inhibited for a long time if a temporary measure or device implemented in order to carry out a test or maintenance operation was forgotten. An analysis in the more general context of improving the quality and safety of maintenance operations had nevertheless shown that use of temporary measures and devices could not be completely avoided, but that they must be subject to particularly strict management procedures giving preference to all the simple measures providing substantial safety improvement, for example making a temporary measure or device easily visible by using a bright colour. A temporary modification of the functional state of the facility must not be introduced unless it is absolutely essential. In the case under discussion, the only reason for installing the temporary measure was to continue the test in order to meet the schedule, which is against the rules set by EDF in 1994.

23.2. Events related to internal hazards

23.2.1. Risk of common-mode failure due to internal flooding

▶ Ingress of hot water into the four process instrumentation system (PIS) rooms resulting in transmission of spurious reactor trip (RT) and safety injection (SI) commands

(Nogent Unit 1 – September 2005)

On 30 September 2005, Nogent-sur-Seine nuclear power plant Unit 1 was restarting after its refuelling outage. The steam generators were supplied with feedwater by the emergency feedwater system (EFWS). At 07:00 on 30 September 2005, the switch-over of the steam generator feedwater supply from the EFWS to the main feedwater system (MFWS) began, according to operating instructions. Nine minutes later, faults were observed on the leak detector of steam generator 1. The investigations conducted by the facility operator led to the identification of hot water flows into the rooms housing process instrumentation system equipment of the two emergency-supplied electrical trains A and B. These flows caused faults in the reactor protection system and the nuclear instrumentation system, which sent spurious reactor trip (RT) and safety injection (SI) commands and spurious alarms. The alarms triggered the on-site emergency plan, with mobilization of the emergency response teams until reactor unit fallback to a safe state and connection of the residual heat removal system (RHRS).

The initiator of the event was a human error: failure by the shift crew to close the MFWS blowdown valves at the 'steam clamp'[662]. Startup of turbine-driven feedwater pump 2 with the blowdown valves open resulted in hot water at about 110°C being conveyed to the steam clamp room through the blowdown lines.

Analysis of the aspects relating to human and organizational factors identified failings in work preparation, schedule management and work execution during conditioning of the MFWS turbine-driven feedwater pump.

The consequences of the event were aggravated by construction faults in the steam clamp room (see Figure 23.3). The facility operator identified two water flow paths from the steam clamp sumps to the electrical building:

– through the seal between the reactor building (RB) and the electrical building (BL). By design, this seal is protected from water influx by a parapet higher than the electrical building peripheral wall. During construction, the parapet was lowered over a length of about one metre. The water was able to flow over the lowered part into the space between the two buildings, and through the seal between them in places where its protective putty layer had been cut out for an assessment;

– along the wall of a sump in the non-leaktight steam clamp room and some of the electrical penetrations. The rising water level in the sump designed to collect dripping from the MFWS and EFWS drains resulted in overflow into a second sump connected to the first. The second sump was not leaktight, allowing water infiltration through the thermal insulation and via non-leaktight electrical penetrations into the rooms at the level below.

The nonconformities identified showed that water flow paths could lead to a common-mode hazard (trains A and B) for electrical equipment important to safety, compromising the separation of the electrical trains. Nevertheless, given the short duration of exposure to the wet environment and the rapid activation of drying

[662] 'Steam clamp' is the term used for the zone delimited by a metal structure that provides shelter from bad weather and the cold for the parts of the steam generator feedwater supply pipes and steam dump pipes (shaped like clamps) located between the reactor building and the turbine hall.

and smoke venting, the influx of hot water into the process instrumentation rooms did not affect the short-term reliability of the electrical equipment located in the rooms.

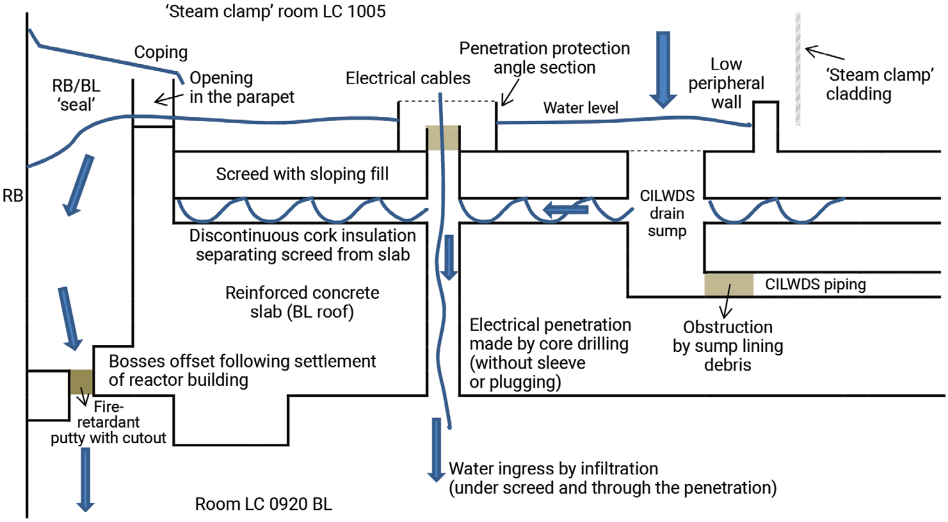


Figure 23.3. Vertical section view summarizing the water flow paths during the Nogent-1 incident that occurred on 30 September 2005. Jean Couturier/IRSN (source EDF).

This event showed the need to verify:

- the safety demonstration of studies on a high-energy line break in the steam clamp,
- the adequacy of measures taken against the risk of flooding in the electrical building and the control room in the event of line break in the steam clamp or on the electrical building roof.

In conclusion, this event shows that the combination of several mutually independent faults could have led to an unforeseen situation which might have been highly detrimental to reactor safety. The event was explained by a human error with consequences that were amplified by construction faults, some of which had been present for over 17 years. Nevertheless, the event would have been avoided had any one of these faults not been present. Consequently, at the design stage, this event would have been considered highly improbable. This also demonstrates that safety also depends on the facility operator's ability to maintain the facility in a state of full compliance, even though some faults or degradation may appear to be without consequences, in principle. This event has been considered generic for the different reactor series by EDF corporate services and has been classified as a core damage precursor.

23.2.2. Risk of failure due to fire

▶ Outbreak of fire at a reactor coolant pump (RCP)

(Penly Unit 2 – April 2012)

In the night of 3-4 April 2012, Penly nuclear power plant Unit 2 was generating power. The 'lift'[663] pump on the motor lubrication system of reactor coolant pump 1 (RCP 1) started up for an unexplained reason (equipment function or human intervention). Neither startup of the lift pump, nor its continuous operation until automatic shutdown of RCP 1 at about midday on 5 April, were detected by the control room operators. Insufficient tightening of a bolt on one of the system flanges led to an oil leak.

Before automatic shutdown of RCP 1, an alarm indicating a low level in its lubricating oil tank appeared in the control room. Two minutes later, fire alarms were activated by detectors located in the rooms housing RCP 1: oil leakage close to very hot components (about 300°C) caused outbreaks of fire. Twenty minutes later, the shutdown sequence of RCP 1 was automatically triggered by an alarm indicating high temperature of the upper thrust bearing of the motor, due to loss of a significant amount of the motor oil. Shutdown of RCP 1 was followed by reactor trip. The operators controlled the reactor according to the emergency operating procedures.

While RCP 1 was shutting down, the seal 1 leak-off line[664] was automatically isolated because of a high leak-off flow rate, probably due to damage to seal 1. However, cold water injection at the seals of the four RCPs was not interrupted, including for RCP 1, which was shut down, where the pressure of the injected water was consequently transferred to seal 2. At about 18:00, the facility operator, concerned that any failure of seal 2 could lead to a loss-of-coolant accident situation (as seal 2 was subjected to high pressures compared with its normal operation), decided to reopen the seal 1 leak-off line to the chemical and volume control system (CVCS) in order to relieve some of the pressure on seal 2.

As previously, the seal 1 leak-off isolation valve received another automatic isolation command because of the high leak-off flow rate. When it was closed again, the isolation valve was no longer leaktight, probably due to particles from damaged seal 1. An unsuccessful attempt to reopen the valve then caused reactor coolant leakage, which was collected in a nuclear vent-and-drain system (NVDS)[665] tank designed for

[663] The bearings of each RCP in operation are lubricated by an oil system; an additional 'lift' high-pressure oil injection system ensures there is an oil film on the RCP thrust bearing before and during startup, as well as when the motor stops.

[664] The three successive seals of the RCPs must ensure that the reactor coolant system is sealed tight. Sealing is obtained by injecting cold water into the seals to act as an obstacle to the hot reactor coolant. Through the resulting three successive controlled leakage stages, the seals lower the pressure from the RCS level (155 bars) to atmospheric pressure.

[665] This system collects liquid and gaseous effluent, produced by nuclear pipelines and systems, which may contain radioactive contamination.

this purpose. The debris produced also released loose matter throughout the CVCS, for example, in the seal water return filter at a SEBIM^{TM} relief valve and at a containment isolation valve. The transients led to a temperature exceeding 110°C in certain pipe segments, which were equipped with valves that were not qualified to operate at this temperature.

Application of the emergency operating procedures gradually reduced the reactor coolant leakage through seal 2 by depressurizing the reactor coolant system. Unit 2 reached a stable shutdown state during the night of 5 April. The event had no environmental consequences.

Origin of the oil leak

During expert investigations on RCP 1, it was observed that a flange seal in the lift pump oil system was no longer in its initial position. A tightening check on the four screws of the faulty flange found insufficient torque on the screw closest to the leak. After disassembly of the piping, inspection of the seal found that it was properly seated, but that it was completely cut near the screw that was insufficiently tightened.

The hypothesis put forward by EDF was that prolonged operation of the lift pump combined with insufficient torque on a flange screw would have led to excessive deformation of the seal and its rupture, resulting in an oil leak.

Origin of the damage to seal 1

An increase in the seal 1 leak-off flow rate and a reduction of its head loss were observed, indicating significant opening of the seal. The damage to the seal was confirmed by the RCP expert investigation. This anomaly appeared to be linked with the concomitance of the oil leak and the inappropriate presence of a lock plate in the mechanism of seal 1. The lock plate found in seal 1 was evidence of non-quality maintenance practices during the standard replacement of seal 1 during the refuelling outage in 2009. The procedure used for installing the seal was not able to detect this foreign matter. The procedures and French national maintenance rules were updated to include a check to ensure that seal 1 slides freely in its groove. No effects of the non-quality maintenance work conducted in 2009 were detected until 2012. The deviation was detected in April 2012 in conjunction with the low oil supply related to the leak.

Corrective actions undertaken by EDF

Following the event, RCP 1 at Penly nuclear power plant Unit 2 was replaced, except for the pump volute, and the tightening of all the oil system flange screws was checked on all the RCPs of both Penly plant reactors. EDF then produced a partial reactor coolant system requalification programme and implemented it before restarting Penly Unit 2. The programme defined the actions to be taken (visual inspections, dye penetrant testing, metallographic replicas, cleaning and replacement of parts) following the event.

In addition, to determine the exact causes of the equipment failures, EDF conducted expert investigations on RCP 1, the electrical cubicle of the lift pump, and the valves located on the seal 1 leak-off lines of the four RCPs. Tightening of the oil system flanges was also checked during the refuelling outages of the French nuclear power reactors to collect operating experience feedback.

▶ Fire following overheating of cables supplying power to the circulating water system (CWS) pumps

(Cattenom Unit 2 – May 2004)

On 16 May 2004, when Cattenom nuclear power plant Unit 2 was restarting following a refuelling outage, an electrical cable fire broke out in a fire stop opening between the electrical building and the turbine hall accommodating, among others, the 6.6 kV electrical cables. The fire was detected by an alarm indicating an insulation fault in the 6.6 kV LGB switchboard, followed by a fire alarm.

Following these alarms, the facility operator applied the emergency operating procedures, and facility operation was switched to procedure I4D ('Total loss of train A due to fire'). In accordance with procedure I4D, the facility operator disconnected the train A electrical switchboards and the off-site power lines. The train B power supply was then provided by the train B emergency diesel generator until the power supply through the auxiliary transformer was restored.

The fire was caused by overheating of the cables in a cable feed-through opening (see Figure 23.4) supplying 6.6 kV to the circulating water system (CWS) pumps to the condenser. These cables were undersized (only in the Cattenom nuclear power plant) with respect to the nominal power of the pumps (9 MWe). In addition, the opening concerned was closed at both ends, preventing removal of the heat radiated, resulting in heat build-up causing charring of the cables. The power of the pumps circulating water to the condenser in the other 1300 MWe reactors is lower (nominal power 5 MWe).

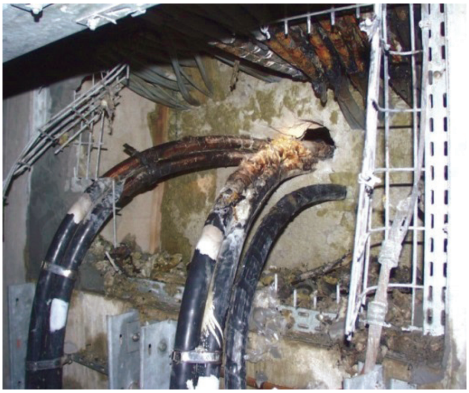


Figure 23.4. 6.6 kV cable trays after the Cattenom-2 event on 16 May 2004. EDF.

The facility operator replaced the cables on the four Cattenom nuclear power plant units using a different routing scheme with two cables per phase, and eliminated the 'oven' effect in the electrical openings concerned by removing one of the walls, as only one was necessary.

This event revealed anomalies in the design of electrical distribution and cable routing, in particular running cables belonging to train B through the rooms of train A without specific protection.

The first complete application of the emergency operating procedure I4D in a real situation showed that the procedure defined by EDF for managing a fire leading to total loss of train A was generally satisfactory.

Analysis of the aspects related to human and organizational factors revealed failings that resulted in delays in calling off-site emergency services, application of operating procedure I4D and calling the National Emergency Command Centre in order to initiate the on-site emergency plan. Corrective actions were introduced following the event.

This was one of the most significant precursor events in 2004.

23.2.3. Risks associated with the use of hydrogen in 900 MWe reactors

The risks associated with the use of hydrogen in nuclear power plants call for close attention at the design stage and during operation, in order to avoid any ignition or explosion of a hydrogen-air mixture; aspects of this topic are discussed in Section 11.7 of Chapter 11 on internal hazards.

▶ Uses of hydrogen in a nuclear power plant

From an on-site gas storage zone, pure hydrogen is piped from cylinders to the turbine hall for injection into the turbine generator rotor cooling system, and to the nuclear auxiliary building for injection into the reactor coolant system to compensate for the effects of water radiolysis[666].

In addition, the hydrogenated gaseous effluent produced during reactor operation is periodically removed from the reactor coolant system by the nuclear vent and drain system (NVDS), first to a buffer tank, then to the gaseous waste treatment system (GWTS) tanks. In addition to hydrogen, this effluent contains fission gases (xenon and krypton) and nitrogen. It should be noted that one GWTS system is used by two 900 MWe reactors.

[666] Under the action of radiation, water breaks down into hydrogen and oxygen, which is a strong oxidant. This process, called 'radiolysis', favours corrosion in the reactor coolant system. When the reactor is operating, hydrogen is injected into the reactor coolant system to reduce the oxygen content through recombination, thus reducing corrosion effectively.

▶ Risks associated with using hydrogen

At room temperature and pressure, hydrogen is a colourless and odourless gas. In certain conditions, given the presence of oxygen in the air, ignition of a nitrogen cloud formed by leakage from a pipe or a tank could result in an explosion: in dry air, hydrogen deflagration can occur at concentrations ranging from 4% to 75% hydrogen by volume, while detonation, much more destructive, can occur at concentrations ranging from 18% to 59%. The safety consequences of a hydrogen explosion in the nuclear part of a power plant can include release of radioactive substances into the environment, or loss of equipment necessary to maintain the reactor in a safe state or to fall back to a safe plant shutdown.

▶ Events and lessons learned

The risks associated with hydrogen were highlighted in particular by an event that occurred at the Chinon nuclear power plant in 1998, discussed in Section 11.7 of Chapter 11 on internal hazards in a nuclear reactor. The personnel tasked with internal inspection of a valve on a pipe in the system supplying hydrogen to the nuclear auxiliary building of Unit B4 mistakenly opened the corresponding valve of Unit B3, which was in operation, resulting in a major hydrogen leak. Assessment of the increase in probability of core damage in this situation showed that this event had to be considered as a very strong precursor (possibility of an explosion causing a loss-of-coolant accident, with safety injection failure due to damage to the SIS pumps – see Figure 23.5 below).

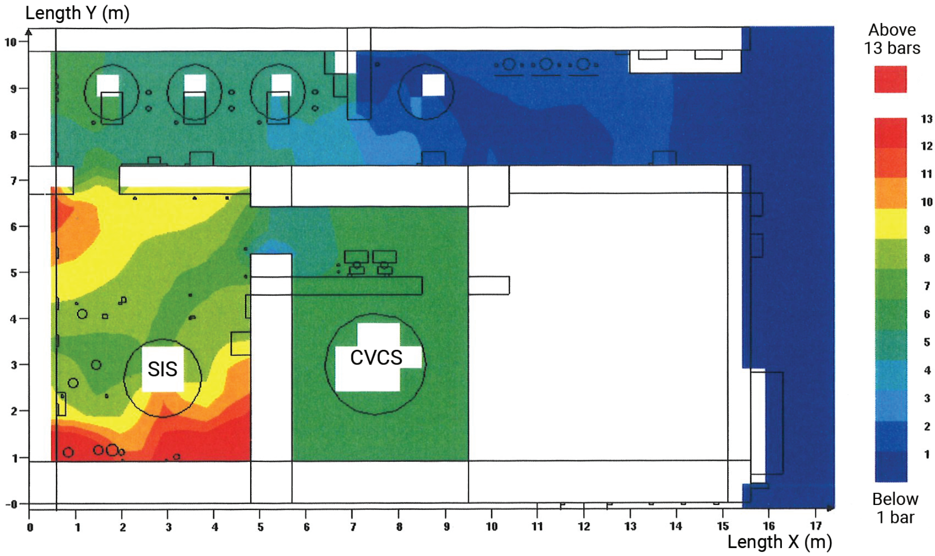


Figure 23.5. IPSN computer simulation of the potential consequences of hydrogen ignition in the room containing an SIS tank and explosion of the dispersed hydrogen showing the same characteristics (leakage rate, rooms involved) as the Chinon Unit B3 event; the pressure values obtained are 7 bars on average and 13 bars in the room accommodating SIS components. IRSN.

Following this event, EDF undertook a series of checks on the condition of the pipes conveying hydrogen in the four units of the Chinon nuclear power plant. The facility operator observed that the carbon steel double walls[667] of hydrogen distribution pipes were corroded; the double wall sections were consequently replaced.

A local-reading nitrogen pressure gauge was added in the double walls of the hydrogen distribution pipes on the sites, with a daily reading by field operators, and a hydrogen detector was added in the room housing the SIS tank containing the boric acid solution at 21,000 ppm boron. In addition, management of the alarms indicating hydrogen in the rooms was revised in order to improve reactivity of the shift crews.

In September 2005, Unit 1 of the Fessenheim nuclear power plant was operating at power and preparatory work for a maintenance and refuelling outage was in progress. This work included planned operations to prepare the transfer of hydrogenated effluent from the reactor to the nuclear auxiliary building ventilation system, which dilutes the effluent before it is discharged to the atmosphere. In this context, a pipe spool is used to feed hydrogen or air to the chemical and volume control system tank (volume control tank, VCT). When the reactor is at power, the line-up provides a hydrogen blanket in the tank. At the start of the reactor outage, the pipe spool is flushed with nitrogen to avoid formation of hydrogen-oxygen mixtures. Following nitrogen flushing, the pipe spool is switched over to the compressed air system for flushing with air. The personnel carrying out the operation loosened the pipe spool used to feed hydrogen to the volume control tank while the unit was still at power. The hydrogen gas escaped with a deafening hissing noise and the explosimeter tripped an alarm. The explosimeter reading was at the lower explosive limit, corresponding to a hydrogen content of at least 4%. The personnel lost no time in leaving the room. An alarm was displayed in the control room. A few minutes later, the personnel realized that the pipe spool was still conveying hydrogen, and they re-entered the room wearing ear protection and re-tightened the flange of the pipe spool. The room door was left open in order to ventilate the room.

As in the case of the Chinon Unit B3 event in 1998, the lack of appropriate information in the alarm sheet impeded timely intervention. Actions raising personnel awareness of the risks associated with hydrogen during work on pipes conveying hydrogen at pressure were recommended. In addition, functional identifiers were assigned to the pipe spools, and operations on hydrogen systems were divided into several sessions, all to be carried out with the reactor shut down.

In June 2006, when Gravelines nuclear power plant Unit 5 was restarting after a refuelling outage, an inadvertent safety injection signal was transmitted. The reactor configuration led to isolation of the CVCS charging and letdown lines, startup of the low-head safety injection pumps, and activation of the residual heat removal system relief valves. Operation of the relief valves, designed to limit the pressure in the CVCS

[667] The pipes have a double wall up to their entry into the nuclear auxiliary building, except at the Fessenheim power plant.

volume control tank, for 3 h caused vibration in the pipes, resulting in two cracks. The estimated flow rate through these cracks was 30 L/h. Any new stress on the line downstream of the relief valve on the minimum flow line of the charging pumps would have risked total rupture of the pipe, which could have resulted in an explosion in the room if the maximum volume of hydrogen in the tank had been released[668]. The explosion would have resulted in the loss of both safety injection trains, as they are located in a room adjacent to the room were the tank is located. This event showed that operation of the safety injection function as prescribed by the procedures when the reactor coolant system is single-phase (pressurizer filled with water when the reactor is shut down) was unsatisfactory. The event showed the need to replace the charging pump minimum flow line safety relief valves with a different model to avoid line cracking and the associated explosion risks.

In June 2007, while Chinon nuclear power plant Unit 4 was at power, the facility operator received an alert indicating excess hydrogen consumption. Investigation showed that a portion of the hydrogen piping was heavily corroded. Inspection of the hydrogen piping of the other three units at the facility resulted in similar observations. A maintenance policy on pipes conveying hydrogen had been issued in the second quarter of 2007, but had not yet been applied in full at the date of the event. Examination of the defective Unit 4 piping revealed generalized corrosion with some perforations, but no risk of sudden rupture. However, if the piping had ruptured completely, there would have been a risk of damage to equipment important to safety because of the explosive atmosphere in the room. This event was a reminder of the importance of the maintenance on pipes conveying hydrogen. When the same piping in Unit 1 was being repaired, some personnel with inadequate knowledge of the state of the unit cut into the pipe when it was still conveying hydrogen. Although the safety consequences were minor in view of the volume of hydrogen remaining in the piping, this event showed the need to add these pipes to the list of sensitive equipment covered by the maintenance operation reliability improvement actions and practices developed by EDF.

In 2008, the French Nuclear Safety Authority (ASN), with IRSN support, conducted inspections on several power plants to verify their management of explosion risks. Most of these inspections showed that the measures taken by EDF were incomplete with regard to the regulations applicable to pipes containing explosive substances. Consequently, on 13 November 2008, ASN took two decisions regarding this subject. The first required that EDF improve explosion risk management in its nuclear power plants within three months. The second, taken in view of the situation observed during inspection of the Cruas-Meysse nuclear power plant, gave EDF formal notice to restore facility compliance with regulations within three months.

Analyses of the above events show that hydrogen release in rooms could have serious consequences for both personnel and equipment important to safety located in these rooms or adjacent rooms. They also show that hydrogen release can have

[668] It should be noted that this type of event may occur in rooms without hydrogen detectors.

diverse causes (human, organizational or documentary). Hydrogen risks must therefore be examined closely and analysed specifically.

23.3. External hazards: events related to periods of extreme cold

▶ Multiple instances of unavailability resulting from extreme cold

(Chinon Unit B3 – January 1987)

The 1987 cold spell caused an event in Chinon Unit B3 that may be described as a precursor to more serious situations.

On 12 January 1987, French electricity consumption was very high because of the weather conditions. Three of the four units of the Cordemais thermal power plant located near the mouth of the Loire tripped simultaneously. The cold itself was the cause of these failures.

The major voltage drop of the 400 kV electricity distribution grid in western France resulting from the tripping of these three units in a period of high electricity consumption caused seven nuclear reactors and two other fossil fuel units to trip. The tripped reactors included Chinon Unit B3, following activation of protection against excess current in the AC generator rotor.

The reactor power supply was switched over automatically to the auxiliary 225 kV line, which was itself weakened. The reactor trip caused the steam generator emergency feedwater system (EFWS) to start up.

The voltage provided by the emergency-supplied electrical switchboards decreased, but the emergency diesel generators did not start up automatically, because their connection threshold setting was too low. The generators were started up manually by the operators. The two EFWS motor-driven pumps tripped because of overcurrent (compensating the low voltage). The four component cooling water system (CCWS) pumps also tripped successively. Various contactors were damaged and removed from service, interrupting the heat tracing[669] function that maintains the temperature of certain cabinets and pipes.

The generators and pumps were successively returned to service by the operators before the main electrical power supply was available again, after a 15-minute interruption.

One hour before this event, the operators had discovered that the outside temperature (-10°C), combined with a sustained wind, had caused the EFWS water tank resupply pipe to freeze. The tank level fell during 4 h. The unit was brought to pressure and temperature conditions allowing connection of the residual heat removal system (RHRS).

[669] System maintaining equipment at an adequate temperature using electrical heating cables.

Over the same period, two water level sensors on the fuel pool cooling system (FPCS) tank were found to be frozen, which could have prevented the safety injection sequence from functioning correctly in the context of a loss-of-coolant accident (not switching to water recirculation would entail a risk of loss of safety injection). The sensors and resupply of the EFWS tank were returned to service after a few hours.

The next day, the operators noted that two steam line safety relief valves were leaking. Once again the cold was to blame, in combination with the interruption of heat tracing. Once again, performing the appropriate operations restored a normal situation.

During the same period, work was needed to clear the pumping station water intake, where icing threatened to block water inflow.

All these failures had a single cause: the prevailing weather conditions over the entire region. The fact that they did not all occur at the same time was pure chance.

▶ Icing on the pumping station anti-intrusion grille

(Chooz B – January 2009)

The Chooz B nuclear power plant, located in the Ardennes region, has two 1450 MWe units (B1 and B2) that use once-through cooling with water from the Meuse River.

On the morning of 9 January, after a very cold night (-15°C), a field inspection observed a difference of about two metres between the water level of the Meuse River and the water level of the intake canal (between the anti-intrusion grille and the pumping station). This difference resulted from the formation of ice on the anti-intrusion grille separating the river channel and the intake canal. The situation led to partial blockage of the flow to the water intake and a water level in the intake canal below the minimum level required. Nevertheless, this low level did not cause any malfunctioning of the pumps on the cooling system for systems important to safety (the essential service water supply pumps). However, a slightly lower water level in the intake canal could have had significant safety-related consequences by affecting the performance of these pumps on either or both of the Chooz B units. Some time in the morning, a tear in the fabric of a filter panel on the train B chain screen was observed. The fabric tear caused clogging of the heat exchangers between the essential service water system (ESWS) and the component cooling water system (CCWS), followed by a rapid fall in the discharge flow rate of the train B ESWS pump, which nevertheless did not compromise the effectiveness of CCWS cooling.

If the cooling water supply had undergone significant degradation, the two units of the Chooz B nuclear power plant could have experienced a total loss of cooling water.

The icing that occurred at Chooz B is referred to as ‘frazil ice’, consisting of viscous ice crystals that take form in a slow turbulent flow at temperatures slightly below 0°C for fresh water. Taking into account the low flow rate in the channel at the water intake at Chooz B, frazil ice formed in the channel, with ice crystals agglutinating on the upstream side of the grille bars, facing the flow, in a continuously increasing mass. This accumulation, in both in width and depth, continued until ‘bridges’ were formed between the adjacent bars, obstructing the flow of water. A wall of frazil ice eventually formed over the entire thickness of the grille bars.

As soon as the grille icing was detected, the facility operator took action to break up the ice. This resulted in a quick return to the normal pumping station feedwater situation.

To avoid the risk of obstruction by ice inside the pumping station, the design of the Chooz B nuclear power plant included a winter recirculation system to maintain a water temperature above 3°C at the pumping station inlet. However, as the risk of rapid obstruction of the intake canal grille had not been considered, no protection system had been provided upstream of the grille. This event underlines the importance of not only ensuring compliance with safety requirements as regards potential weather hazards, such as frazil ice, but also periodically reassessing the adequacy of the associated protection measures.

To avoid further obstruction of the grille, the facility operator installed a mobile hot water system upstream of the grille and a video monitoring system. Furthermore, the ‘extreme cold’ specific operating rule, applicable from the end of 2009, now required permanent monitoring by the facility operator, including hot water recirculation as a frazil ice countermeasure when the temperature of the Meuse River falls below 1°C and the air temperature below 5°C, and field inspections to check temperature, as well as special ice removal equipment.

▶ Freezing rain leading to loss of the main off-site power lines

(Paluel nuclear power plant – December 2005)

The Paluel nuclear power plant has four pressurized water units. The power generated is transmitted (see Figure 23.6) by the 400 kV transmission lines through the main transformer (MT). A step-down transformer (ST) supplies the on-site 6.6 kV system. The two emergency-supplied trains have separate 6.6 kV supplies (LHA on train A and LHB on train B) emergency-supplied by a second off-site source, the auxiliary transformer (AT)[670], and by an on-site source, a diesel generator. There is also a 380 VAC emergency-supplied power distribution system using a turbine generator driven by steam from the steam generators.

On 30 December 2005, it was raining, temperatures were below zero, and a strong wind was blowing over the Paluel nuclear power plant. The wind passing over the discharge ponds near the 400 kV power transmission switchyard produced a salt mist

[670] A specific feature of 1300 MWe units is that their auxiliary transformer is supplied by the unit having the same parity (even or odd) in plants with four units and by the twin unit in plants with two units. If off-site power is lost, reactor islanding is initiated by tripping the line breaker, reducing the generator load to the power consumed by the auxiliary systems.

that was deposited on the insulators. These particular weather conditions contributed to the formation of a partial ice coating on the insulators[671] of the 400 kV substations. Electric arcing on the main transformers of the four units resulted in rupture of the corona rings[672] and caused successive shutdown of the main power lines of the four units and loss of the auxiliary transformers. Three units successfully switched over to islanding, but the attempt failed for Unit 2. Unit 2 tripped after the turbine tripped due to overspeed. Unit 2 continued to be supplied by the diesel generators and operated in thermosiphon mode (natural convection).

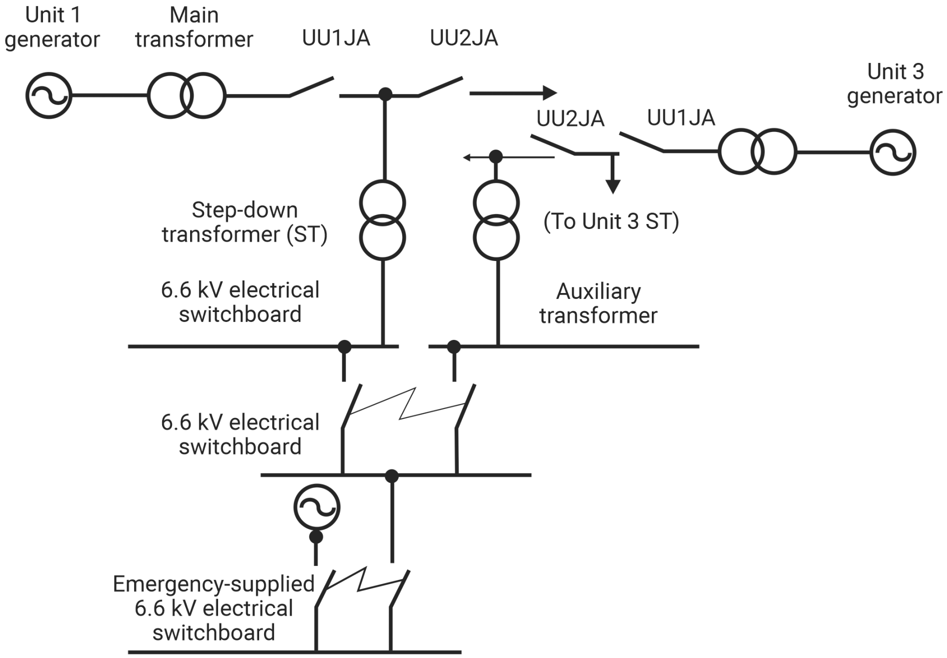

Unit 1 generator
Main transformer
UU1JA
UU2JA
Unit 3 generator
UU2JA
UU1JA
Step-down transformer (ST)
(To Unit 3 ST)
6.6 kV electrical switchboard
Auxiliary transformer
6.6 kV electrical switchboard
Emergency-supplied 6.6 kV electrical switchboard

Figure 23.6. Electrical power supply of the Paluel nuclear power plant units (example of Unit 1). IRSN.

The design of the power distribution system of French nuclear power plants is such that freezing rain established a common-mode failure situation resulting in the loss of both off-site power sources to the four units. The probabilistic safety analyses showed that this event had to be considered as precursor of a core damage accident.

[671] The insulators protect against overvoltage. They consist of a defined number of stacked porcelain disks arranged in such a way that the leakage path prevents any electrical arcing.

[672] The corona rings are secured to the top of the insulating discs, on each phase of the main transformer, for protection against electrical arcing. They maintain dielectric strength, especially during lightning surges and in rain, and reduce the corona discharges due to ionization of the air molecules, and the associated losses and interference. There are two corona rings on each insulator.

It appeared that this event was not covered by the modifications incorporated in 1984 following a similar event. Moreover, in this event, icicles formed between the insulator discs, degrading insulator performance. The insulation was further degraded by sea salt spray trapped within the icicles as they formed. The ice shortened the natural leakage path of the insulators, generating voltage build-ups. The power line breakers opened to eliminate the fault.

Chapter 24

Enhanced Protection of Estuary and River Sites

Flooding at the Blayais Nuclear Power Plant and Obstruction of a Water Intake at the Cruas-Meysse Nuclear Power Plant

This chapter focuses entirely on two significant key events caused by 'external hazards': the partial flooding of the Blayais nuclear power plant site during a storm that hit France in late December 1999, and a build-up of plant debris that obstructed the water intake of two of the four reactors at the Cruas-Meysse nuclear power plant at the beginning of December 2009.

Many lessons were learned from these two events. In particular, the partial flooding of the Blayais nuclear power plant site led to an in-depth review that was much more far-reaching than the ten-yearly safety reassessments, which provided the opportunity to incorporate new knowledge and data in hydrometeorology. The review focused on the protection of sites from flooding risks of any kind (high river levels, rainfall, etc. and their possible concomitant occurrence) and also led to significant enhancement of this protection.

24.1. Partial loss of engineered safety systems following flooding of the Blayais nuclear power plant

▶ Brief reminder of the events and their effects

The Blayais nuclear power plant is on the eastern bank of the Gironde estuary, north of the city of Bordeaux. It has four 900 MWe units.

During the night from 27 to 28 December 1999, a strong depression and very strong winds – with gusts reaching about 200 km/h – caused very high water levels in the Gironde River, coinciding with high tide. The existing protection, in particular the peripheral dykes, could cope with a 'static' water level of the height reached during that night, but not with waves generated by swell in the estuary. The wind swell led to the protective dyke being breached by water and to partial flooding of the nuclear power plant. Because of the direction of the wind and waves, it was mainly units 1 and 2 that were affected by the flood; very little water entered the buildings of units 3 and 4.

The exceptional weather conditions also caused disruption to the electricity grid, leading to total loss of the 225 kV auxiliary power supply to all reactors for about 24 h and loss of the 400 kV main power supply to units 2 and 4 for several hours.

The water entered drainage channels, flooding the basements of the administration buildings and the general auxiliaries building. The water then spread into the buildings of units 1 and 2 through doors and other openings, reaching the basements of the electrical buildings, the connecting corridors to the pumping stations, and the basements of the adjacent buildings and fuel buildings (see the simplified diagram in Figure 24.1).

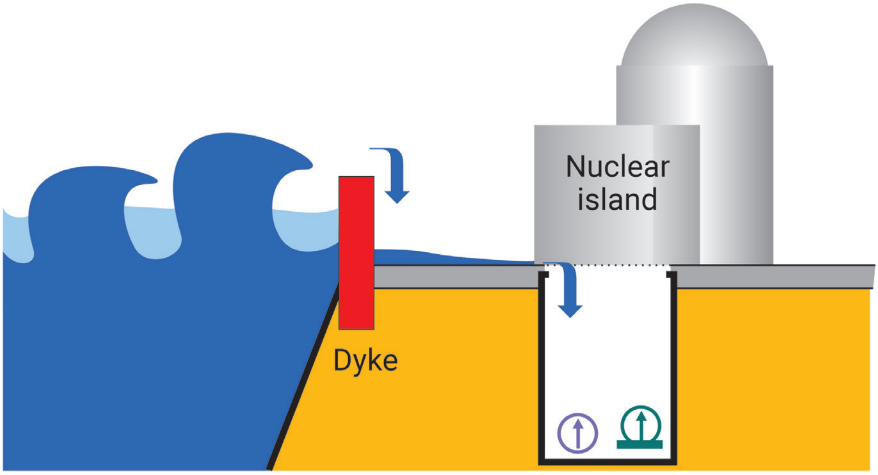


Figure 24.1. Diagram of flooding at the Blayais nuclear power plant in December 1999. IRSN.

The flooding led mainly to the loss of the following equipment and systems:

- at Unit 1, the two pumps on train A of the essential service water system (ESWS). The two pumps on train B remained operational. At Unit 2, the four ESWS pumps remained operational. The reactor coolant fluid continued to circulate in units 1 and 2, since one reactor coolant pump remained in operation;
- at both units 1 and 2, the two trains of the low-head safety injection system (SIS) and the containment spray system (CSS).

During the first few hours of the event, backup teams were unable to reach the site from outside the nuclear power plant because of damage caused by the storm (flooded access roads, many fallen trees, etc.). The nuclear power plant personnel began pumping operations in the first few hours of 28 December. The water pumped out was discharged into the Gironde River after its radioactivity level had been checked. Pumping ended late in the evening on 29 December.

Following the flooding, the personnel from units 1 and 2 proceeded to bring the reactors to a normal shutdown state with cooling of the reactor coolant system provided by the steam generators (normal shutdown using SG).

Once this state had been reached, the operator's main concern was to guarantee the long-term operation of each reactor's emergency feedwater system (EFWS) by continuously replenishing the water reserve in the tanks of these systems from the facility's demineralized water reserves and by operating the demineralization station. Units 1 and 2 were thus maintained in a 'normal shutdown using SG' state and brought to the conditions for connection of the RHRS, pending stabilization of the national electricity grid, availability of all the facility's electrical power systems (off-site power supply, electrical panels), availability of the entire ESWS and requalification of one train on both the SIS and CSS, where the pumps had been flooded. These conditions were necessary to guarantee sufficient availability of the engineered safety systems so that eventually a refuelling outage state could be reached, allowing the condition of the reactors to be examined thoroughly. Units 1 and 2 eventually reached the conditions for a refuelling outage on 18 and 15 January 2000, respectively.

Unit 3 was maintained in a normal shutdown state with cooling provided by the RHRS and was not affected by the flooding. Unit 4, which had first been brought into a hot shutdown state, went critical again on 30 December.

The partial flooding of the Blayais nuclear power plant site[673] led to implementation of the on-site emergency plan (Level 2), from 09:00 on 28 December 1999 until 18:00 on 30 December 1999; the national emergency response was set up in the morning of 28 December and was in operation until 30 December. In the morning of 28 December, the most critical phase of the flood, after assessing the situation at Unit 1, it was considered that the operator would have more than 10 h to act before core melt if the EFWS failed. The EFWS, which has two motor-driven pumps and a

[673] Classed as a Level 2 event on the INES scale.

turbine-driven pump – a single pump is enough for reactor cooling – showed no signs of failure throughout its operation.

The partial flooding of the Blayais nuclear power plant site was considered a precursor to core damage, with conditional probabilities of core melt (depending on the additional failures considered) of several 10^{-3} (in assessments made by Électricité de France [EDF] and IPSN).

Protective dyke design

The level initially used to design the protection structure of the Blayais nuclear power plant site was 5.02 m NGF[674], representing the highest tide level (coefficient of 120) raised by an extra amount to take into account weather conditions (wind, low pressure systems, etc.) and local topography. The dyke was an earthwork protected on the Gironde River side by rockfill consisting of stone blocks. Along the riverside, the dyke level had been set to 5.2 m NGF; along the site side, it had been set to 4.75 m NGF. Studies conducted by EDF, presented in the 1998 safety analysis report for the Blayais nuclear power plant, led to a revision of the water level considered for site protection purposes, and it was changed to 5.46 m NGF. EDF had planned to raise the height of the dyke to 5.70 m NGF, but the work required, originally planned for 2000, had been postponed to 2002.

During the storm in late December 1999, heaving water submerged the nuclear power plant platform, coming in mainly on the north-west side of the dyke. The rockfill on the dyke was displaced by the passing water, which levelled it on the side facing the Gironde River. Water on the site reached a height of about 30 cm in the north-west corner of the site.

Platform submersion and the water course

The water flowed preferentially into the main site gallery through the handling ports in the plates covering the gallery, and through gaps left by deformed sheet-metal panels. This main gallery, situated outside the buildings, almost completely encircles them. The water flow that entered the gallery, reaching up to 30 cm high, was estimated to be between 20,000 and 40,000 m^3/h. This value was corroborated by the estimate of the volume of water pumped out of the buildings (approximately 90,000 m^3 of water was discharged between 27 December 1999 and 1 January 2000) and by the fact that the presence of water on the site was observed for approximately 2 h.

Corrective measures, lessons learned

Following this event, the location of all French nuclear power plants was reassessed to check their compliance with existing 'baselines' and to rapidly implement operating experience feedback from the event. Work to bring facilities back into compliance was carried out where necessary.

[674] *Nivellement général de la France* (the French general datum system).

In terms of operating experience feedback, the main lessons learned from the partial flooding of the Blayais nuclear power plant site were as follows:

- the effects of swell, although taken into account in the design of coastal power plants, had been underestimated in the case of this facility bordering an estuary;
- the facility's protective dykes proved inadequate and poorly suited to the weather conditions that caused the flooding;
- as described above, several rooms at units 1 and 2 were flooded, particularly rooms housing equipment important to safety such as the pumps in train A of the essential service water system for Unit 1, and at units 1 and 2, the two pumps (trains A and B) of the low-head safety injection system and the two pumps of the containment spray system; during the event, these pumps did not need to operate because the accident situations for which they are required did not materialize. Moreover, the facility's off-site power supplies were partially and briefly lost during the event;
- the facility's flood alert system (based on the water level at the mouth of the estuary) proved inappropriate for the climate conditions that caused the flooding;
- the flooding temporarily prevented access to the site (for about 10 h), due to flooding of the access roads or obstruction of those roads by debris;
- there were problems with detecting and assessing the presence of water in certain flooded buildings (in particular the building containing the engineered safety pumps).

The safety functions (reactivity control, residual heat removal, confinement of radioactive substances) continued to be performed throughout the flooding episode by the equipment that remained available (in particular the steam generators and train B of the essential service water system).

Action plan implemented based on the lessons learned from the event

Although the event on the Blayais site did not itself lead to a hazardous situation for the public or the environment, it did reveal potential ways in which the safety level could be degraded, affecting in some cases all the reactors on a single site. EDF and the safety organizations therefore felt that it was essential to learn all possible lessons from this event to prevent it happening again, either at this site or at other nuclear power reactor sites. Accordingly, in addition to implementing urgent measures at the Blayais plant, EDF defined and implemented an action plan to reassess and where necessary upgrade the external flooding protection measures at the 19 nuclear power reactor sites. As of 2000, IRSN was heavily involved in assessing this action plan and the changes made at facility sites to improve their protection. The improvements made to achieve better management of flood-related risks were carried out in several stages.

Stage one: short-term actions (emergency measures) taken at the Blayais site and first reflections on questions of principle (for all NPPs)

Obviously, the priority was to take appropriate measures at the Blayais site to ensure its protection: revision of the water level taken into account in dyke design (to include swell), raising the height of the existing dyke, adding rockfill, improving the alert system, inspection of facilities, repair of damaged equipment, etc.

In addition, after reviewing the approach taken previously, EDF proposed a new approach to protecting facilities from external flooding, taking into account the different possible causes of flooding (high river, sea or estuary levels, dam failure, swell, local wind waves, prolonged or storm-related torrential rain, rupture of a system or structure, mechanically induced wave, high groundwater levels, etc.) and combinations of these causes. At the end of 2001, the safety organizations decided that, in principle, the proposed new approach was generally satisfactory.

Stage two: a more in-depth definition of the new approach

From 2002 to 2007, EDF's new approach and its implementation were defined in depth and adapted to the different nuclear power plants; improvements were made to this approach and the assumptions used, studies were carried out to adapt implementation to each of the 19 nuclear power plant sites, and upgrades or changes to be made at the sites were defined.

The studies on implementation of the approach at the 19 nuclear power plant sites represented a large amount of work for EDF because each site is different and has different vulnerabilities, and there are more than ten different flooding phenomena to consider, as well as different combinations of these phenomena.

There were two parts to EDF's approach:

- for sites where external flooding protection could not be provided by raising the nuclear island platform, but was based instead on civil works (dykes or walls), the approach consisted of checking the height and strength of these structures in light of the reassessed water levels. If necessary, these structures would have to be raised, strengthened or in some cases reinforced by additional measures, adding a margin when determining the height of the protective features in relation to the reassessed water levels;
- for all sites, the equipment required to allow the reactors to reach and maintain a safe state was identified. This equipment had to be kept safe from flood water. Accordingly, for each reactor, the approach aimed to provide a watertight volume encompassing all such equipment, referred to as the 'watertight volume approach'. This volume generally included the rooms contained in the infrastructure, given the risks related to rising groundwater levels. Its height, however, depended on site vulnerability to external flooding (the 'watertight volume' could be limited to infrastructure at a site where the nuclear island platform was located high enough above the body of water requiring protective

measures). Any risk of bypassing the physical protection measures (dykes, ‘watertight volume’, etc.) had to be addressed.

Stage three: definition of changes and execution of work

Application of the new protection approach led EDF to carry out major works, proportionate to the variable vulnerability of the 19 nuclear power plant sites, including:

- changes to civil works, for example the construction, reinforcement or raising of the height of peripheral protective structures (dykes, walls), work to dewater the site platform and seal the rooms to be protected (by providing a sealing solution capable of keeping out potential water ingress and appropriately qualified for the relevant water load);
- installation of flood alert systems combined with operating procedures to take preventive action where necessary (closing access to the ‘watertight volume’ by installing stop gates at buildings forming the superstructure, closing valves on infrastructure pipes, etc.), and monitoring the state of the nuclear power plant during flooding;
- installing water level sensors and the associated alarms (on condenser pits, pumping stations, etc.) in various rooms;
- installing additional stationary or mobile pumping equipment (sump pumps in rooms containing the ESWS or other equipment important to safety);
- making physical changes or changing operating strategy at certain nuclear power plants to reduce the risks of losing off-site power supplies or clogging of water intakes by debris during flooding; for example, at the Belleville-sur-Loire nuclear power plant, measures were taken on in-coming power lines to prevent the loss of facility power supplies.

After analysis, the safety organizations considered in 2007 that the measures implemented or planned at the different facilities represented significant progress in terms of safety and gave them a satisfactory level of protection against external flooding risks. However, further studies appeared to be necessary, for example, for sites in the Rhone valley, because of structures outside the sites (water-control dykes and structures) that were not operated by EDF, but could have an impact on the reaches of flooding.

Since the end of 2014[675], all measures implemented to take into account operating experience feedback from the partial flooding of the Blayais nuclear power plant site are now operational across the entire nuclear power plant fleet.

[675] This deadline was set by ASN after the flooding entailed by the Fukushima Daiichi nuclear power plant accident in March 2011.

Towards reinforced and more uniform flood protection practices at nuclear facilities: development of a guide applicable to all basic nuclear installations

Following the partial flooding of the Blayais nuclear power plant site, it became apparent that measures to ensure flooding protection at other nuclear facilities (research reactors, laboratories and industrial facilities) needed to be reviewed. In March 2007, the French Nuclear Safety Authority (ASN) informed the various operators that they must adopt an approach to taking into account external flooding risks that was consistent with the one implemented by EDF.

For this purpose, a working group was set up in 2006, led by ASN and IRSN, consisting not only of different nuclear facility operators, but also other experts in the fields of hydrology, hydraulics and meteorology. Its long-term objective was to produce a guide on taking into account external flooding risks at all basic nuclear installations and harmonizing practices in this area; it was designed to replace fundamental safety rule RFS I.2.e issued in 1984, which covered the protection of pressurized water reactors against flooding. This publication is presented in Section 12.4.

24.2. Total loss of heat sink due to clogging of filter drums by a massive influx of plant matter at the Cruas-Meysse nuclear power plant

Icing on the anti-intrusion grille at the pumping station of the Chooz B nuclear power plant in 2009, described in Section 23.3, was caused by a period of extremely cold weather leading to frazil ice formation on the grille.

The event described below had similar consequences for the facility's equipment but was caused by an influx of debris, which clogged the pumping station.

Following a rise in the flow of the Rhone River, a very large mass of plant debris that had accumulated on the river bed and banks over the previous months clogged the inlet of the pumping station at units 3 and 4 of the Cruas-Meysse nuclear power plant overnight from 1 to 2 December 2009. Clogging of the pre-filtration screens by plant matter led to a drop in water level at the pumping station. When the low flow alarm was triggered on the train in service (train A) of the ESWS used to cool systems important to safety[676] in Unit 4 (reference A4 in Figure 24.2), the operator applied the procedures defined for this type of situation. The operator gave the command to trip Unit 4 and switched system cooling for items important to safety to train B (item B4).

[676] In the event of loss of the ESWS, which makes direct use of river or sea water after filtration, the intermediate cooling circuit, the CCWS, is no longer cooled and thus cannot in turn cool equipment in the reactor engineered safety systems. The refuelling water storage tank (RWST) is then used for temporary cooling of the CCWS. At the same time, the emergency feedwater system (EFWS) is responsible, as an engineered safety system, for residual heat removal. The EFWS water reserves can undertake residual heat removal for a period estimated to be long enough to restore cooling water.

Following this switch-over, however, the operator observed that train B was also no longer operational due to clogging of the water intake.

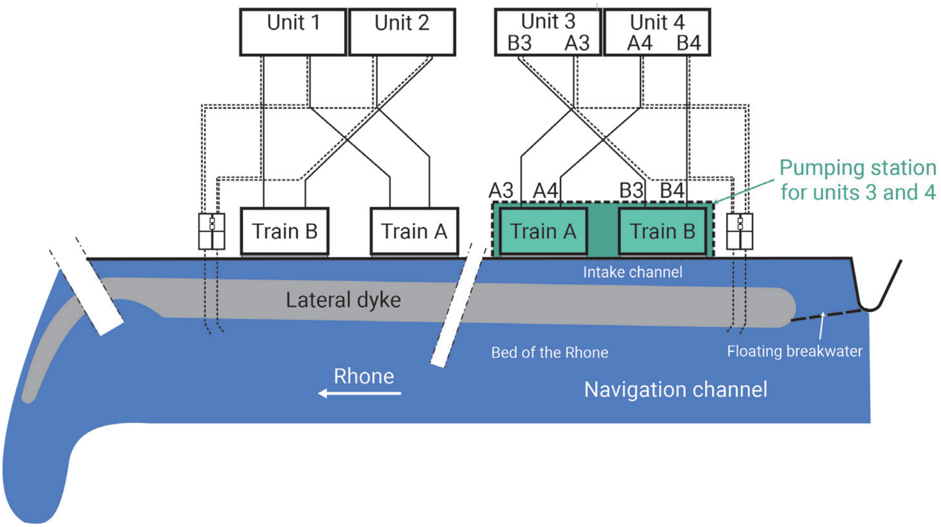


Figure 24.2. Configuration of trains A and B of the ESWS systems at the Cruas-Meysse nuclear power plant. IRSN.

There was therefore a simultaneous loss of two trains for cooling systems important to reactor safety, leading subsequently to a total loss of heat sink.

The total loss of heat sink for Unit 4 lasted about 10 h. However, throughout the event, the reactor core was cooled by the steam generators, which remained available. Unit 4 was then maintained in a safe state by applying procedures where the fuel pool cooling system water reserve is used as an emergency heat sink. At the same time, the operator cleaned the filtration devices in the pumping station and the ESWS/CCWS heat exchangers. After this cleaning operation, the two trains for cooling systems important to safety were once again available early in the morning of 2 December 2009.

Operation of the three other reactors at the Cruas-Meysse facility was also disrupted, but to a lesser extent. Because units 3 and 4 share a pumping station, alert signals appeared on 1 December for Unit 3. Train B of the ESWS for Unit 3 (reference B3 in Figure 24.2) was declared unavailable late in the afternoon on 1 December, and this lasted until the next morning. However, train A of Unit 3 (reference A3) remained available.

The pumping station for units 1 and 2 experienced a smaller influx of debris, though this still caused the loss of train B of the ESWS for Unit 2 on 2 December. Throughout this period of unavailability (approximately 6 h), the operator applied the appropriate operating procedures and made sure train A remained available by cleaning the pre-filtration screens more frequently at the pumping station intake.

Obstruction of the pumping station intake was caused by an aquatic plant known as ‘Nuttall’s waterweed’ (see Figure 24.3). This plant, which originated in North America, appeared in the early 1980s in Swiss lakes, then in the Rhone River from the 1990s. It has extremely long, fine stems (up to 3 m in length) covered with small leaves. Because of the increase in the Rhone River’s flow rate, the operator of the dam upstream of the Cruas-Meysse nuclear power plant had redirected the flow from the east channel to the (natural bed) west channel where the power plant is located. This caused the Rhone River to carry away a large mass of debris formed by the waterweed, which had accumulated for several months on the bed and banks of the Rhone River.

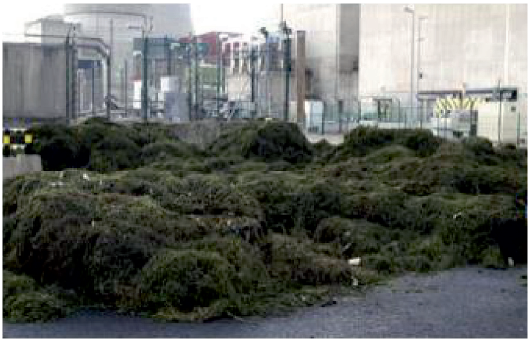


Figure 24.3. Heap of vegetation that caused clogging at the Cruas-Meysse nuclear power plant in December 2009. EDF.

This event emphasized the fact that the rapid occurrence of unforeseeable external hazards can affect all reactors on a single site. Despite all the means provided for monitoring, protection, pre-filtration and filtration at its pumping stations at the time of the event, the Cruas-Meysse site simultaneously suffered the partial loss of heat sink at two units (2 and 3) and total loss of heat sink at one unit (4).

Faced with potentially recurrent clogging, an appropriate safety approach would be to ensure that, regardless of the circumstances, the reactors could always be shut down and maintained in a safe state, thereby ensuring that the power supply to the ESWS pumps would always be available. It therefore seemed necessary to reinforce the preventive measures already in place at the water intake and the pumping stations by adding alert and detection systems as well as protection systems. Inadequacies and shortcomings were identified in the pumping station design: there was no water level measuring instrument at the ESWS pump suction intake (which would have detected a significant drop in level); the secondary system cooling pumps were not preventively triggered in clogging configurations; the screen cleaners designed to clear pre-filtration screens in a normal operating situation could not cope with a massive influx of clogging material while the pumps were operating at full flow.

As indicated in Chapter 13, the risk of total loss of heat sink at French nuclear power reactors has been taken into account in France since the 1980s, in particular with the development of the H1 operating procedure. In application of the procedures for a total loss of heat sink, the event required the thermal inertia of the refuelling water storage tank (RWST) tank to be used, and this proved effective at limiting the CCWS temperature to about 15 degrees until the heat sink was restored. This real accident situation also demonstrated the beneficial contribution made by the mass of water in the spent fuel pool (in the Fuel Building) which, by limiting heating of the CCWS, reduced the urgency of using the thermal inertia of the RWST, the countermeasure required by procedures.

Finally, loss of heat sink at all the reactors on a site, a situation which could have arisen during the event at Cruas-Meysse, was given particular attention during the periodic review associated with the third ten-yearly outage of 900 MWe reactors. The review led to the enhancement of measures capable of controlling this risk, in particular ensuring availability of the SG feedwater system water reserves.

The event at the Cruas-Meysse nuclear power plant in 2009 was a reminder of the importance of periodically re-examining water quality, taking into account changes in the natural environment and checking that existing procedures and measures are adequate.

Chapter 25
Taking into Account Human and Organizational Factors in Facility Operation

The importance of human and organizational factors in ensuring the safety of nuclear power reactors is highlighted in Chapter 4 of this book, and their incorporation at the facility design stage is developed in Chapter 16. They also need to be taken into account in all aspects of operation. This is the focus of the present chapter, which provides general principles and concepts, as well as the approaches taken, illustrated by examples from operation of French nuclear power reactors.

The sections below address the following subjects: skills management by facility operators, safety management, human and organizational factors in facility operation and maintenance activities, and finally issues related to the management of subcontracted activities.

The discussion presents the measures implemented, along with their successive improvements. It shows how facility operators must constantly give close attention to human and organizational factors in all matters involving operation.

25.1. Skills management

The management of individual and collective skills is a key contributor to the safety of nuclear facilities. For a facility operator like Électricité de France (EDF), skills management has various facets: ensuring that new personnel who will perform activities important to safety acquire the skills they need to do so effectively; maintaining the skills of personnel trained in this way over time and in an evolving technological environment; anticipating personnel turnover in such a way that sufficient expertise is maintained during critical periods, such as those marked by a high number of retirements; and capitalizing on the knowledge and know-how acquired over time and passing it on to the appropriate people.

In addition, facility operators must ensure that the contractors they select are capable of performing the required services under satisfactory safety conditions.

25.1.1. Historical background

From the 1980s onwards, French safety organizations gradually turned their attention to skills management, covering areas as broad as training methods, staff certification provisions, recruitment planning, and even the incorporation of lessons learned from significant events into training. Several meetings of the Advisory Committee for Reactors were dedicated to this matter. On occasion, preparatory work for these meetings included studies undertaken by working groups (J. Bourgeois from 1980 to 1981, and G. Y. Petit[677] from 1984 to 1986) involving facility operators, safety organizations and institutions outside the nuclear sector, while international practices were also taken into consideration. In several cases, operating experience feedback highlighted gaps in personnel skills. One example, as seen in Section 22.2.1, is the analysis of the event that took place in March 1990 involving the sensors on the water-level measuring system in the Unit 2 pressurizer at the Cruas-Meysse nuclear power plant. This analysis showed that the event was due to poor understanding of the systems and underestimation of their complexity; although an operating procedure had indeed been modified to take into account the installation of new sensors, the authors of the document did not have detailed knowledge of the systems. In 1991, the Advisory Committee for Reactors formulated recommendations, which were echoed by the Directorate for the Safety of Nuclear Installations (*Direction de la sûreté des installations nucléaires*, DSIN), with the aim of significantly reinforcing training activities. These covered the definition of required skills, the recruitment and qualification of personnel responsible for training, procedures for individual skills assessment, certification procedures and training for maintenance personnel.

In the mid-1990s, EDF made strategic decisions aiming to give local site management greater freedom to organize and take action on developing and maintaining skills and to involve front-line managers more closely in such activities. The goal was to provide a solution more suited to local needs in terms of training and certification. However, the inspections performed by the inspectors of basic nuclear installations to evaluate the effects of these changes in the field highlighted difficulties in the deployment of these decisions: shortcomings in local organizations and in coordination between national (corporate) level and the sites, and difficulties faced

[677] Professor (CEN Bordeaux-Gradignan), at the time a member of the Advisory Committee for Reactors.

by sites in transitioning from a knowledge transfer approach to a skills development approach – the latter point representing a profound change. In 1999, these observations led DSIN to seek additional information and action from EDF.

In the mid-2000s, the safety organizations performed a specific evaluation of EDF's approach to managing personnel skills and certification in light of the projected growth in the retirement rate – and the resulting high turnover of operating and maintenance personnel – expected by 2010.

The case studies carried out by IRSN (in preparation for the 2006 meeting of the Advisory Committee for Reactors on skills management) covered the following jobs or specializations: control operator, 'first-line manager' within a department responsible for automatic control systems, test technician, supplier surveillance supervisor and the reactor core operations manager. Some of the lessons learned from this exercise, notably in relation to strategic workforce planning, are detailed below.

The issue of skills is also regularly addressed in the examination of activities important to safety (reactor operation in the control room, equipment maintenance, fuel handling operations, etc.), in the root cause analysis of a significant event, or even in evaluations of cross-disciplinary issues such as safety management or supplier surveillance. Since the Fukushima Daiichi nuclear power plant accident in 2011, this issue has also been considered alongside the size of the workforce and the training (including practical exercises) required to enable personnel to deal with an extreme event.

25.1.2. Managing training

The general personnel training process implemented by facility operators has four main goals: to enable personnel to initially acquire the skills required (following recruitment or an internal transfer), to maintain these skills (in the case of technological developments, for example), to ensure that skills are adapted to changes in facilities and their operating methods, and to transfer skills (which also covers capitalizing on knowledge and know-how). Skills are not, of course, limited to theoretical knowledge (such as knowing how to read and apply a procedure), but are largely developed through practical, operational understanding associated with experience of work situations, ultimately enabling personnel to adapt to a variety of situations, some of which may be unexpected. This capacity to adapt also assumes the ability to draw on a range of skills, whether collaborating on an activity or tackling a new problem.

EDF has allocated significant resources to training its thousands of employees working in the nuclear sector, with, at national level, a department in charge of managing training and training tools such as control room simulators and training sites for maintenance activities.

After initial general training, EDF personnel receive further training as part of their professional development. In this respect, EDF runs a programme targeting particular skills (which forms part of strategic workforce planning, discussed in more detail below), notably in order to address the transition phase created by the retirement of the 'builder' generation and to train newcomers. In addition to the standard training received by all new employees, ‘first-line managers’ set out a professional development plan for their colleagues by selecting the most suitable training activities based on the existing skills of new employees and the skills they need to fulfil their respective roles. As a complement to theoretical training, EDF has taken measures such as:

- mentoring with recognized peers to learn technical tasks;
- real-life training on simulators in work teams for training in uncommon or rare situations, such as those requiring the use of incident or accident procedures;
- drills on training sites for certain activities.

The various training tasks are evaluated to ensure that they are relevant to the desired objectives. Lastly, the different training activities completed by personnel are recorded in individual professional development logs (formerly known as training logs), which are checked during inspections by the French Nuclear Safety Authority (ASN).

Since the Fukushima Daiichi nuclear power plant accident, EDF has introduced specific measures to train and prepare its personnel for extreme events. In particular, these aim to give personnel the individual and collective capacity to cope with stressful situations. As an example, the training and preparation for teams in the Nuclear Rapid Response Force (see Section 36.6.6) takes inspiration from best practice in civil protection: ‘tactical reasoning methods’, drills for large-scale emergencies involving multiple EDF entities (operating crews, local and national emergency response teams, etc.), emotion management techniques and the introduction of unforeseen events into drills to develop teams’ adaptation and resilience capabilities.

25.1.3. Strategic workforce planning

EDF has gradually structured and formalized its strategic workforce planning processes (*Gestion prévisionnelle des emplois et des compétences*, or ‘GPEC’) to ensure that it has, at all times, the skills required to meet production and operational safety objectives. With this approach to planning, the aim is to ensure that skill requirements can be identified between two and five years in advance. Once these requirements have been identified, the actions needed to fulfil them (recruitment, training, acquisition of know-how and career management) are determined in turn, taking into account the skills already available within the company.

First of all, identifying the skills required involves drawing up a list of needs for the various disciplines, roles and responsibilities (operation, maintenance, supervision, supplier surveillance, etc.). Implemented in the field by ‘first-line managers’, this exercise is largely based on interviews and observation of the actual work performed by personnel. The results may be formalized in ‘skill mapping’ tools that can be used at both local and national level. This type of representation is accompanied by an inventory of the skills actually available, together with the objectives for each skill and department, which facilitates management of the skills that need to be built up over the medium term. This is notably done to secure skill acquisition, especially where a long time period is required for professional development. The use of skill maps also helps establish the number of personnel who are operational or undergoing training. Succession tables aim to determine any handover needs generated by retirement or other types of departure, so that optimal 'skill incubators' can be designed.

In addition, EDF informs contractors of the expected volume of activities and draws up part of the corresponding contracts on a multi-year basis.

It is also interesting to note that facility operators have worked in cooperation with the national education system to provide information on professional opportunities in certain areas of competence (welding, for example) and offer apprenticeship contracts.

Beyond the management of individual skills, skill maps are also a useful tool in evaluating the state of skills available within a work group. In particular, for operating crews, they can be used to spot any lacking skills so that appropriate steps can be taken to obtain them (through personnel transfers, training, etc.). Lastly, these maps and follow-up actions are examined during inspections by ASN.

25.1.4. Personnel certification

In a French nuclear power plant, all personnel performing activities important for 'protected interests' (as defined in regulations) must have the appropriate level of certification authorizing them to carry out these activities. This involves nuclear safety and radiation protection in particular.

'Nuclear safety certification' was introduced by EDF in the early 1990s. Nuclear safety certification for personnel constitutes recognition, by management, that an individual has achieved the qualifications needed to perform activities important to safety within a defined scope (job, unit, activity, equipment or process, and duration of certification). Certification is issued based on an evaluation of the level of skills acquired by the individual through training and professional experience. In order to ensure that personnel have those skills, managers also observe their performance in work situations and on simulators.

Proof of nuclear safety certification is kept in an individual training log (now known as an individual professional development log) for each personnel member, and certifications are checked regularly. Certification may be withdrawn at any time or suspended temporarily, for example if an individual changes role, temporarily or permanently stops performing an activity, or fails to demonstrate an adequate level of skill.

By signing a nuclear safety certification document for a member of personnel, a manager confirms that the individual does indeed have the skills corresponding to that certification. In turn, personnel members sign the document themselves to confirm that they believe that they have the skills required for certification, accept the responsibilities entrusted to them and agree to work within the defined scope.

At the end of the 1990s, examination of significant events in nuclear power plants brought to light shortcomings in the nuclear safety certification process for personnel. For example, during certain events, it became clear that some operators – despite being certified – lacked experience. Furthermore, during its inspections, DSIN uncovered recurring nonconformities related to certification renewal, indicating a degraded situation. These cases included certification being issued despite personnel not having completed certain compulsory training courses, or several instances of failure to keep individual training logs up to date. In 2000, these observations led DSIN to ask EDF to take steps to ensure that certification documents do indeed guarantee that certified personnel have the qualifications required to perform the corresponding activities. EDF then made efforts to introduce the necessary rigour to the process for issuing and renewing certifications. This point is still checked regularly by inspectors from ASN.

In 2004, EDF decided to enhance the professional development path for young recruits by establishing a progressive nuclear safety certification system allowing them to enter work situations more rapidly.

Lastly, following the evaluation mentioned above carried out in the mid-2000s (see Section 25.1.1), ASN asked EDF to specify how teams would be set up and organized in the event of a one-off, temporary loss of skills[678].

25.2. Safety and risk management

Safety has an essential role in the management of a nuclear power plant. It involves applying technical, human and organizational measures to control risk and maintaining them over time.

25.2.1. Historical background

EDF has been progressively building up its safety management system[679] since the 1970s. Initially based on quality assurance initiatives in line with the Quality Order of 10 August 1984, it was later enhanced with the introduction, in 2014, of an integrated management system compliant with the regulatory requirements of the INB Order of 7 February 2012 (see Chapter 2 and Section 4.6).

The Three Mile Island accident in 1979 and the Chernobyl accident in 1986, in the first instance, led EDF to enhance existing provisions, with a view to improving operator reliability through the introduction of measures to prevent and 'recover from' human errors. This involved, among other things, reinforcing procedures and checks and appointing nuclear safety and radiation protection engineers working in shifts[680] to check that safety aspects were taken into consideration by operating crews

[678] For example, when a control operator is asked to prepare operational activities to be performed during an upcoming unit outage, his or her workload may enter into conflict with the requirement to maintain certification for reactor operation, which requires a minimum number of operating hours per month.

[679] For more information, see *Le management du parc nucléaire d'EDF* (Managing the EDF Nuclear Power Plant Fleet), A. Kenedi and D. Clément, *Éditions L'Harmattan*, 2007.

[680] A single nuclear safety and radiation protection engineer monitored at least one pair of units. The nuclear safety and radiation protection engineers (later known as nuclear safety engineers) initially reported to nuclear power plant management, then to the safety and quality department.

(see Section 32.4.1). With the introduction of the 'operating safety' approach in 1993 and the creation of the role of shift manager (in charge of overseeing safety elements), the nuclear safety and radiation protection engineers became nuclear safety engineers responsible for checking that the operating crews, led by the shift manager, were duly taking safety elements into account. In order to improve redundancy, nuclear safety engineers ceased to work on a shift basis.

At international level, the IAEA published the INSAG-4 report on safety culture in 1991 and the INSAG-13 report on safety management in 1999. In 1997, EDF adopted a safety management policy based on six 'levers':

- risk analysis,
- self-diagnostics,
- self-assessment,
- operational communication,
- the Safety/Availability Monitoring Unit (for retrospective analysis of the conditions and quality of decisions taken),
- an approach to managing delicate transients[681] during reactor operation.

In order to deploy this policy across all its sites (nuclear power plants), EDF relied on, among others, the 'human factor consultants' based at its nuclear power plants since 1993, who assisted with the implementation of initiatives and methods specific to human factors, with a view to improving work situations in particular.

The management policy of the Nuclear Power Generation Division was enhanced in 2004 with the incorporation of process-based management (safety, production, etc.), inspired by the European Foundation for Quality Management (EFQM). The key elements of this policy are given below:

- safety is affirmed as a priority;
- progress loops are set up at each level of the organization (department, site, corporate level, etc.), on the basis of diagnostics shared from operating experience feedback, including 'early warning signs'[682];
- the presence of managers in the field is vital to give structure to productivity and safety requirements that must be integrated into the activity, and also to help solve problems;
- the management of individual and collective skills must be reinforced, especially in the context of personnel turnover.

[681] Transients such as power ramp-up after core refuelling, involving numerous parameter adjustments and special monitoring to ensure that the reactor does not exceed the specified operating domain (and potentially trigger reactor trip).

[682] This involves identifying, based on observations during daily operation, underlying elements that could be improved proactively to prevent a 'bigger' event.

The improvement of safety performance varies from one site to the next (it is useful to recall, in this respect, the introduction in 2000 of reinforced oversight by the French safety authority for certain facilities, such as Dampierre-en-Burly). Managerial actions to ensure that the improvement of safety performance is sustainable over the long term and consistent across all sites have been set out in a joint safety management 'baseline'. In this context, the role of human factor consultants has been reinforced to include contributions to operating experience feedback from events; providing support and advice to operating units, teams and project structures; and the development of knowledge in the field of human factors. In addition, since the end of 2006, EDF has introduced measures to improve the reliability of work activities (see Chapter 4).

In 2011, a comprehensive, multi-year project entitled 'Generation 2020' was set up by EDF, with the major goals of increasing the reliability of equipment, infrastructure and organizations, and improving professionalism. Three key principles of safety management are emphasized by EDF: leadership, skills development and personnel engagement, and result-based and process-based management (production, safety, etc.) with a view to continuously improving performance.

Lastly, internal controls constitute an important component of safety management. As seen above, in the 1980s, EDF introduced nuclear safety and radiation protection engineers, later known as nuclear safety engineers, followed by an 'independent safety review team'[683] with a double role: to perform safety analyses independently from the operating crew, and to provide technical support to operational departments where needed (for example, to apply operational limits and conditions in complex situations), in all areas where safety is concerned.

In-house inspections take place at various levels of the organization, from the local level constituted by operators in the field, using methods such as self-checks by the operator and cross-checks by a peer, all the way up to corporate level. The measures implemented by sites are regularly checked by internal auditors from the site safety and quality department, and inspected by the Nuclear Inspectorate of the Nuclear Power Generation Division. In addition, the Inspector General for Nuclear Safety and Radiation Protection at EDF produces overall assessments of the state of the nuclear power plant fleet in terms of safety and radiation protection[684] on behalf of the corporation's chief executive officer. Sites are also evaluated during peer reviews under the WANO scheme or missions by the IAEA Operational Safety Review Team (OSART) – see Chapter 3 for details.

25.2.2. Decision-making and safety

Decision-making must give top priority to safety. Decisions in this instance may concern technical equipment or processes, human activities, risk management

[683] The independent safety review team is made up of the nuclear safety engineers and based in the safety and quality department, which also hosts the quality process auditors.

[684] The annual reports of the Inspector General for Nuclear Safety and Radiation Protection are available to the public.

processes or industrial performance, or – more broadly – the organization of work and personnel. All parties involved in the decision-making chain, particularly managers, must constantly balance multiple goals and restrictions (nuclear safety, availability, environment, radiation protection, occupational safety, etc.), make compromises and set priorities in terms of resources. Decisions may be influenced by many factors, including situational, relational, organizational, policy-related and cultural factors.

EDF has therefore placed a special focus on decisions that call for achieving a balance between safety and production, with the establishment of the independent safety review team, as mentioned previously. As a company, EDF constantly strives to stay competitive, for example by running regular optimization and maintenance programmes (discussed further in Chapter 26), reducing reactor outage times, rationalizing procurement of equipment and services, and reducing costs and the size of the workforce (particularly for maintenance). In 2004, EDF became a partially privatized limited company in a European context of deregulation of the electricity market and the gradual opening up of utility companies to competition. Organizational analyses of industrial accidents in many sectors[685] have shown that the pursuit of competitiveness must be counterbalanced by reinforcing safety management measures. There are several questions to consider in this respect:

- Is priority really given to safety in the compromises made every day at nuclear power plants?
- In a constantly changing organizational and managerial environment, does safety retain an operational meaning for operators?
- Do the measures in place and the general corporate context provide sufficient capacity for identifying improvements in safety-related areas?

To evaluate the responses that these questions might receive, IRSN conducted case studies in preparation for the 2008 meeting of the Advisory Committee for Reactors on safety management in a competitive context at EDF (following its 2004 privatization). These studies identified factors that contribute to a satisfactory compromise in terms of safety and those that do not. For example, these factors may include the diversity of skills or responsibilities united within a steering committee, the level of redundancy of information channels, or even the degree of cohesion within a group given time pressures and the approaches taken by different parties.

The development and application of indicators by EDF managers in their daily work may be useful, as long as these are regularly reviewed in terms of their weight in decision-making and management, and in terms of managers' critical reflections on the meaning of the indicators themselves.

In addition, it has been possible to evaluate the understanding of safety at an operational level through targeted interviews with decision-makers and operators, thereby

[685] For further information, see the report of the inquiry into the Columbia space shuttle disaster (*Columbia Accident Investigation Board Report*, 2003) and *L'accident et l'organisation* (Accident and Organization), M. Llory and R. Montmayeul, 2010, *Éditions Préventique*.

obtaining their 'impression' or point of view regarding the effectiveness of risk control measures and the constraints experienced. Areas covered have included the day-to-day role of management; time-related aspects, particularly the time available for diagnostics and decision-making; the question of skills; the use of 'baselines'; the preparation and execution of work activities; operating experience feedback; and organizational and technical constraints.

Despite the variability of situations encountered in the different nuclear power plants, IRSN identified particular strengths during its case studies, such as EDF's capacity to use 'project mode' to decompartmentalize its organization, the complementary nature of risk-control measures, and the mobilization of multiple skills to diversify viewpoints in the decision-making process. However, certain vulnerabilities were also observed, such as the complexity of rules and instructions, the large number of processes that burden operators, difficulties in developing and applying organizational experience feedback, the shortcomings of internal checks at certain sites.

The analysis performed in 2008 led ASN to issue several requests to EDF regarding decision-making and compromises. In this respect, the establishment by EDF of the Observatory on Safety, Radiation Protection, Availability and Environment (an extension of the Safety/Availability Monitoring Unit mentioned above), which analyses situations that have required making compromises, was considered to constitute an appropriate tool for improving decision-making.

25.2.3. Risk analyses applied to work activities

Risk analyses are an essential tool in risk control. Their purpose is to identify risks in advance, for example those associated with a maintenance activity, and then establish provisions or 'countermeasures' to control these risks. The analysis process involves engineers and set-up technicians from the various disciplines in question, as well as operators, which helps ensure that the latter understand the risks in question. Just like any initiative rolled out in the field, the risk analysis process must be managed at national level and supported at site level in order to ensure that risk analyses are of high quality. The process must also undergo regular assessments.

A review of significant events that occurred between 2000 and 2002 highlighted the difficulties faced by operators in understanding and implementing the risk analysis process; these difficulties were among the noted causes of significant events (three events per year per reactor). Certain failures observed concerned preparations for maintenance operations. In one such case, a risk that had not been identified in the risk analysis during file preparation by the maintenance teams was one of the causes of an event at Chinon B4 in March 2002. Similarly, on 21 January 2002 at Flamanville 2, during a scheduled maintenance operation on the inverters of the LNG 220 V power supply switchboard for the train A Controbloc computer system, an error in the procedure file and the incorrect emergency action led to the simultaneous loss of the train A Controbloc and the 6.6 kV emergency-supplied and non-emergency-supplied train A switchboards. This event, managed using the 'state-oriented' approach, resulted in reactor shutdown, the loss of water injection into the reactor coolant pump seals for more than one hour (the exchanger on the component cooling water system and essential service water system (CCWS/ESWS) for train A being unavailable), and damage to the two pumps on the steam generator emergency feedwater system (EFWS) while power was being restored to the 6.6 kV emergency-supplied switchboard for train A. The risk analysis did not mention the importance of the checks to be performed during the intrinsic requalification of the inverters, or the need to switch the cooling for the common CCWS/ESWS equipment to train B. In some cases, risk analysis had not even been performed, as was the case at Chinon B3 on 29 June 2002, when a periodic test on the main steam isolation valves led to a group 1 event[686]. In other cases, risk analysis has been found to be inappropriate for the situation or operating domain, or the countermeasure itself has proven inadequate.

The review of significant events also brought to light failures to take the risk analysis into account during operations. In one case, an experienced operator did not feel the need to use the operating procedure provided, despite the fact that he was performing the activity in question for the first time. On other occasions, the risk analysis has been rendered inadequate, for example due to adjustments in activity scheduling or changes in the initial conditions of an operation, or due to 'pressure' to reduce the reactor outage time.

Originally envisioned as a 'lever' of safety management at the end of the 1990s, since 2014 EDF has considered risk analyses as a 'lever' for overall operational performance, and they now cover all 'protected interests' as defined in the French Environment Code. While this development seeks to encourage successful integration of the requirements generated after analysing all the risks that need to be taken into account when organizing an operation, it could nonetheless result in giving less attention to the specific analysis of safety risks. To avoid this pitfall, EDF has undertaken actions to accompany this new policy.

25.2.4. Operating experience feedback

Drawing on past experience is a key element of safety management. Operating experience feedback remains a constant source of lessons and improvements – as discussed in chapters 21 to 23 of this book – and has been given close attention by safety organizations since the 1970s. Chapter 21 describes the rules and practices of collecting operating experience feedback involving both 'significant events' and 'relevant events'. This discussion reveals that, although the main principles regarding operating experience feedback were formulated as far back as the 1970s, problems involving the feedback process considered as part of operational risk management were still being experienced in 2009, according to an internal audit conducted by EDF. The company subsequently launched an operating experience feedback improvement programme (the 'OPEX Project'), which introduced the 'corrective action programme' (inspired by US practices) and allocated means to recruiting resources for implementation.

[686] The notion of 'group' is described in Section 20.2.1.4.

In addition to events that uncover faults or deviations, a wide range of other activities can provide operating experience that points out useful lessons and improvements. In any case, regardless of the activities under consideration, it is important that operating experience feedback does not focus solely on the technical perspective, but is applied in an integrated approach that also covers human and organizational dimensions.

It is useful, for example, to collect both positive and negative feedback in the field during operating or maintenance activities, and to analyse this information in terms of work planning and coordination, human-machine interfaces, equipment management, management practices, and so on. This type of analysis serves to identify current measures or 'lines of defence' and evaluate their effectiveness. The analysis of several events can, in certain cases, reveal recurring issues or 'early warning signs' of possible slips in safety management that should be corrected. For example, recurring cases where tools or equipment required for operations are not available may indicate unsatisfactory equipment management, which could lead to taking action to improve organization in the units responsible for managing that equipment.

It is also constructive to regularly examine how operating experience feedback is organized (skills and resources mobilized, processes, etc.) in terms of its potential contribution as well as the limits of feedback tools, while taking into account the rapidly developing information technology resources available in terms of big data and natural language processing. EDF and IRSN have launched trials in this area.

25.2.5. Managing organizational change

EDF has extended its analysis approach focused on human, social and organizational impacts – initially developed for designing technical changes (see Section 16.2.2.) – to cover organizational change as well. It is evident that organizational change temporarily destabilizes an existing organizational system, potentially increasing its vulnerability. Such changes have even contributed to industrial accidents, such as the disintegration of the space shuttle Columbia during its return flight to Earth in 2003.

One example of organizational change is the gradual introduction by EDF, since 2010, of a new structure to improve the management of reactor outages, which mainly consisted in creating Outage Control Centres[687]. One particular aspect of this change involved increasing the hours during which the outage project management team was available by setting up a daily rotation of two different shifts. At shift turnover, staff from other outage project teams was called on, who then set aside the

[687] An outage control centre (in French, *centre operational de pilotage des arrêts de tranches*, or 'COPAT') is set up at facility level for certain scheduled reactor outage phases. It aims to ensure a greater presence of outage project coordinators and decision-makers (by organizing two or three 8-hour shifts, 24 h a day, seven days a week), who previously had only been available during normal working hours during outages.

preparations they had been conducting on other reactors at the facility. This meant that management responsibility was passed on to staff who had not prepared that outage and therefore did not understand all the aspects of the decisions made in the preparation stage, which had taken several months. In 2013, following an examination by IRSN and the Advisory Committee for Reactors of safety and radiation protection management during unit outages, EDF launched a study with a view to introducing, in the medium term, measures and best practices to improve outage control centre operators' understanding of the strategies and choices of those who had prepared the outage.

By applying the human, social and organizational impact approach described above (implemented in 2007), facility managers supported personnel as they learned to function in the new outage control centres, designed to facilitate outage management. In addition, EDF corporate services were granted new resources to support change by providing advice and sharing best practices, which has proven successful. However, given the range of constraints faced by facilities, the latter have not been able to deploy all elements of the new system for managing outages, and have continued to apply a slower – but more cautious and pragmatic – approach to change due to the need to adapt to local limitations. Moreover, in 2012 IRSN observed that different ways of organizing unit outages had been implemented: sometimes the system used an approach based on the working hours of the project personnel who had prepared the outage; in other situations, the system was based on the outage control centre, scheduled for two or three 8-hour shifts. Following the 2013 investigation mentioned above, EDF took measures to analyse the risks associated with these varied management systems to reduce any differences in order to stabilize roles and responsibilities.

In the 2010s, EDF made multiple changes simultaneously in order to improve its industrial performance (see Figure 25.1). Although some changes were staggered over time by corporate services and nuclear power plant management to avoid overloading the workforce, the combined effects of certain changes on work organization, or on the scope of work for certain members of personnel, were not always anticipated and prevented.

Furthermore, it became clear in 2013 that the reactor operation and maintenance context was still undergoing noticeable changes, and would continue to do so, with EDF having to take into account regulatory changes as well as facility ageing, at a time when it was also experiencing significant staff turnover and increased competition.

EDF launched the Generation 2020 and Major Refit projects to control the risks associated with these changes and developments.

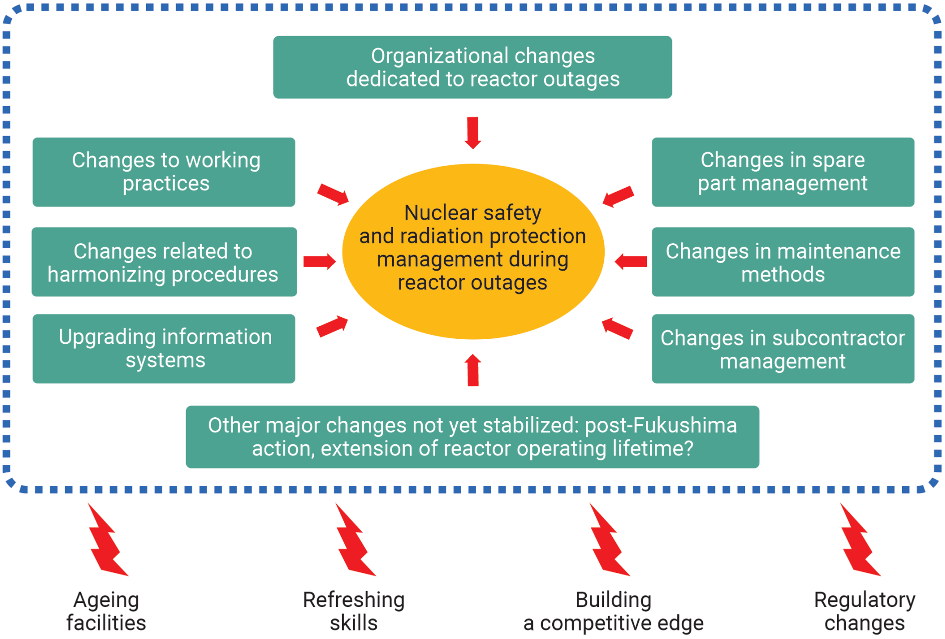

Organizational changes dedicated to reactor outages
Changes to working practices
Changes related to harmonizing procedures
Upgrading information systems
Nuclear safety and radiation protection management during reactor outages
Changes in spare part management
Changes in maintenance methods
Changes in subcontractor management
Other major changes not yet stabilized: post-Fukushima action, extension of reactor operating lifetime?
Ageing facilities
Refreshing skills
Building a competitive edge
Regulatory changes

Figure 25.1. Nuclear safety and radiation protection management during reactor outages in parallel with other changes in 2012. IRSN.

25.3. Managing operational activities

25.3.1. Characteristics of operational activities

Reactor operational activities cover normal, incident and accident situations.

▶ Organization of operation

Since the 1990s, operating crews in nuclear power plants have worked shifts according to the directives of a shift manager (one per pair of reactors, regardless of the series), who is responsible for safety and production at the facility. An operating crew comprises:

- **in the control room:**
  - at 900 MWe, 1300 MWe and 1450 MWe reactors, two operators who manage and monitor the facility: the 'reactor' operator focuses more specifically on the reactor and the reactor coolant system, and the 'steam' operator on the secondary system. At the EPR (Flamanville 3), during normal operation, one 'action' operator performs operation actions under the responsibility of a 'strategy' operator, except during

incident or accident situations, in which the organizational system used is the same as that applied at other reactors;

  - a deputy shift manager: this is the team technical specialist, who organizes and plans operational activities for the shift, checks that they are performed correctly, contributes to fault diagnostics and ensures good coordination between the operating crew and personnel from other disciplines (maintenance, chemistry, etc.). During incident or accident operation (examined in further detail in Chapter 33), the deputy shift manager takes on the role of supervisor, which involves managing and coordinating the actions of the two operators. However, from 2020, an additional operator – the 'lead operator' – is present in each unit to reinforce monitoring during normal operation and provide supervision during incident or accident operation; the deputy shift manager coordinates with the other disciplines;

- **at the tagging office:** a 'tagging supervisor', who deals with requests to remove equipment from operation and tag it appropriately so that maintenance work or inspection operations can be performed under the responsibility of an 'operational safety officer' in charge of the safety of operating and maintenance personnel working on equipment at the facility;
- **in the field:** four or five field operators (per reactor pair) responsible for the direct, local operation of equipment (for example, changing the position of a valve), facility monitoring in the field (local reading of parameter values) and regular patrols (by 'field operators') to detect any anomalies.

This configuration corresponds to the nominal workforce; reinforcements may be brought in during busy periods, for example to restart a reactor after an outage.

In addition to the operating crew, the nuclear safety engineer independently monitors facility safety on behalf of the 'independent safety review team' to which he or she reports. The nuclear safety engineer also takes readings of facility parameters independently of the operating crew in order to develop an 'image' of the state of the facility, which is compared to that of the operating crew on a daily basis.

▶ Operational activities

Normal operation covers a broad range of situations, from facility startup or restart to operation at power, as well as reactor outages required to unload then refuel the core. Operating crews therefore must perform many different activities to meet electricity generation demand while ensuring strict compliance with requirements applicable to nuclear safety and radiation protection as well as safety and the environment. They also need to protect the production facilities. This means they must simultaneously deal with several different types of activity (facility monitoring, periodic tests, follow-up of maintenance activities, management of various contingencies, etc.).

Operating crews are responsible for operating the various systems and equipment items, with the exception of those removed from operation and isolated (tagged) for the attention of maintenance personnel. Daily operation requires making decisions at all levels. In particular, this involves making compromises between safety and production objectives, which are decided by the shift manager in consultation with facility management, the nuclear safety engineer and maintenance services. For example, if a periodic test is scheduled to take place within a limited time slot to avoid damaging equipment important to safety, it may happen that, after the test has started, unforeseen events lead to extending the test. In this case, the shift manager and deputy facility manager must decide whether to continue the test in order to obtain all the information that it is expected to provide, or stop it in order to avoid damaging the equipment.

Far from being reduced to a passive role consisting of monitoring an automatically controlled technical system, control operators are at the centre of varied, often complex situations, and must understand these situations to keep them under control. Whether the operating crew is performing general facility monitoring or completing a specific task, keeping the facility within the authorized operating domain requires its members to have a shared mental 'image' of the state of the facility in order to take effective action. The construction of this image relies on the operators' knowledge, their interactions with other members of the team and the resources made available to them. In this regard, it should be recalled that during the Three Mile Island accident (see chapters 4 and 32), the human-machine interface in the control room led the operators to make a mistake: the control room indicators provided information regarding the valve closing command, not its actual position, meaning that this valve remained open without the operators being aware of the fact. Keeping a facility within the authorized operating domain requires the constant aggregation and processing (interpretation and decisions) of different information from various sources: the control room, information in the field, the knowledge and experience of the team members, communication within the team, interaction between the different disciplines, and so on.

The control room of a nuclear power plant is clearly a central location where safety is considered continuously in daily operations, while ensuring overall efficiency, by means of:

- technical instruments used to provide information on the state of the facility and control equipment operation,
- operating crews providing 24-hour continuous service to monitor and control the facility and check maintenance operations,
- documents specifying the rules to be applied to keep the facility within the authorized operating domain, and describing what should be done during normal operation, incident and accident operation.

Switching from normal operation to incident or accident operation brings about a major disruption. During normal operation, significant changes in the state of the facility (load following, reactor shutdown, etc.) are conducted at the initiative of the operators, who – thanks to their training and operating experience – are best able to manage the usual contingencies. During incident or accident operation, the situation is not the same: depending on the degree of damage to the facility and the kinetics of the incident or accident, the aim is to return the reactor to a safe state more or less rapidly. This is why, whether they are establishing the initial diagnostics of the situation or falling back to a safe state, the operating crew is guided by procedures conceived using an approach based on the physical states of the reactor (the state-oriented approach, described in Chapter 33). These procedures ask the operators, supervisor and nuclear safety engineer to periodically check the state of various important facility parameters (pressure and temperature of the reactor coolant system, reactor vessel water inventory, etc.) in order to change direction, if necessary, towards an operating strategy better suited to the current situation.

Since the Fukushima Daiichi nuclear power plant accident, EDF has established control measures for equipment in the 'hardened safety core' (Section 36.6.5) that would be used in extreme situations, namely to ensure the feasibility of human actions locally and in the control room (additional or robust instrumentation, safe access paths, specific procedures, etc.). This subject will be covered in further detail in Section 25.3.5.

In an emergency situation, the emergency response team (see Chapter 38) provides much broader support to control operators, the supervisor and the nuclear safety engineer at the unit, facility and corporate levels.

25.3.2. Monitoring by the operating crew in the control room

The operating crews in the control room perform general monitoring by checking, at regular intervals, that the values of the main physical parameters characteristic of the reactor state are well within the operating domain authorized in the general operating rules. This is done by consulting the information provided by the instrumentation and control system, displayed on panels (on over 1000 display windows in conventional control rooms[688]) or indicated by visual or audio alarms. The crews also monitor actions taken by automatic control systems (to control temperature and pressure, for example).

It can be difficult, however, to sustain general monitoring activities when it is necessary to perform operating tasks requiring significant attention, or when managing an unexpected situation in real time. The ways in which the task of general monitoring is deferred and responsibilities reallocated between operators must therefore be governed by precise, explicit organizational measures.

[688] Non-computerized control rooms, i.e. those at all reactors with the exception of those in the N4 series and the Flamanville 3 EPR.

In addition, the quality of general monitoring also depends on how ‘peaceful’ it is in the control room. To this end, steps must be taken to ensure that the control room remains a ‘haven of peace’[689], especially during high-risk activities.

It was therefore important to examine the conditions in which monitoring was performed. IRSN presented an evaluation of general monitoring from the control room to the Advisory Committee for Reactors in February 2014, showing that the attention required for general monitoring in the control room sometimes conflicted with management of the other activities to be performed by operators. Yet EDF came up against difficulties in allocating, where necessary, an additional operator to the control room to support the operating crew when the workload so required. This led ASN to request that EDF outline measures to ensure adequate staffing of the operating crew, especially during peaks in activity. As a result, EDF decided, as discussed above, to reinforce the operating crew by introducing a lead operator role to support the two operators, especially with regard to general monitoring.

25.3.3. Compliance with general operating rules

Chapter 20 explained that certain parts (chapters) of the general operating rules are approved by ASN and have regulatory status. It follows that failure to comply with the operational limits and conditions that constitute Chapter 3 of the general operating rules is one of the criteria for reporting a significant event to ASN.

The operating documents used by operators (procedures, worksheets, etc.), which are compliant with the general operating rules, must strike a balance between providing precise instructions to users, and allowing them to use their own judgement to respond appropriately to unexpected situations or those that differ from the standard cases envisaged by the procedure writers. In the day-to-day life of facilities, facility operators must be able to deal with ambiguous or uncertain situations, which may require interpretation of the rules. This interpretation is all the more delicate when performed under the pressure of events, with a need to find a quick response and reconcile contradictory objectives. Such ambiguity may arise, for example, if an equipment item malfunctions in a way that is not straightforward, meaning that the facility operator has to decide whether or not the equipment is available and choose what action to take. Certain situations not covered by the general operating rules may also be encountered by operators, especially if there are multiple cases of unavailability. In addition, general operating rules change regularly and new problems may occur after each updated version, given that they are the basis for drafting many other documents and are applied through documents used by operators every day. The combined effect of these changes may also cause problems in the field.

Difficulty in interpreting operational limits and conditions has been the cause of significant events. As a result, they must be consulted in real time by the operating

[689] EDF talks about creating a ‘haven of peace’ to remind personnel from other areas of the facility that they could be causing a disruption by speaking to control operators in the control room, and highlights the need for a ‘peaceful’ environment.

crew, or even – when necessary – through discussions with other entities at local or national level in order to establish what action to take. In the medium term, this can lead to changes in the operational limits and conditions.

As certain changes to operating rules (general operating rules, including the operational limits and conditions, among others) may be poorly understood by operating crews, EDF completes an analysis of the human, social and organizational impacts (as described in Chapter 16) when any changes are drafted.

25.3.4. Line-up

In a nuclear power plant, the purpose of line-up activities is to make sure that systems for transporting liquid, air, electronic signals or electricity are made available to users. By acting on the position (open or closed) of valves or electrical switches, line-up makes it possible to configure facility systems for various activities: maintenance operations, tests to ensure the availability of electrical circuits, changes in reactor state, etc. Several tens of thousands of line-ups are performed each year across the nuclear power plant fleet, involving a change in position of between one and several tens of components of different types, sometimes located far apart in different rooms or positions. Line-ups are mainly performed by field operators from the operating crews, in liaison (often via telephone) with operators in the control room and tagging supervisors (who coordinate and record tagging operations in the tagging office next to the control room).

Some years, around 30 line-up errors affecting the availability of systems important to safety might be recorded. This is why facility operators need to remain particularly vigilant regarding the organizational system for line-ups and the conditions under which they are performed in order to better understand the root causes of these errors, whether recurring or new, and adopt appropriate measures.

In this respect, it should be noted that line-up is generally a routine or repetitive activity for operators and may be partially automated. It may be carried out in disrupted contexts, for example, during reactor outages, where there might be delays, interruptions or excessive workloads, or even degraded situations in terms of personnel safety, radiation protection or accessibility, requiring an updated analysis of the associated measures.

Line-up errors are often attributed to human errors involving, for example, confusion between different components or rooms, oversights or incorrect adjustments, to name a few. Greater in-depth analysis highlights more profound malfunctions in the organizations or work groups that are responsible, for example, for preparing and executing unit outages, or updating the documents (procedures, plans) used for line-ups, or even in the design of equipment, which may prove – once in use – to be inappropriate for the conditions in which the equipment is used. Errors of this type may lead to differences in how the field operators and control room operators view what might be a rapidly changing situation. One example of this occurred in 1990, when errors were made during line-up of the water level measurement sensors in pressurizers, as described in

Section 22.2.1. These types of line-up error show that communication between the field operators and control operators is a determining factor in making such activities more reliable. In this respect, since the mid-2000s, EDF has implemented practices to improve reliability in operations conducted by humans[690], one of the important aims being to ensure 'structured'[691] communication between operators.

25.3.5. Operation in extreme situations

At the Fukushima Daiichi nuclear power plant, the operating crew and emergency response team were confronted with extremely degraded working conditions, due to the impact of the tsunami in particular, alongside a sequence of unforeseen situations to which they had to adapt very quickly. ASN asked EDF to identify the human actions required to manage extreme situations and to ensure that nuclear power plants were staffed at all times by sufficient numbers of qualified personnel to deal with the extreme situations taken into consideration as part of the complementary safety assessments (notably loss of the power supply or heat sink). With a view to increasing the robustness and resilience of operating crews (in terms of adaptation capacity) when they are managing extreme situations, since 2014 EDF has carried out real-life tests for operating crews on full-scale control room simulators. As indicated above, EDF also decided to reinforce operating crews by adding a lead operator. At the request of safety organizations, additional tests are being designed, in particular to improve the simulation of degraded operating conditions and interactions with emergency response teams. Some of these tests will only be possible when the hardened safety core equipment is fully installed, i.e. after 2020.

25.4. Management of maintenance activities

As noted in Chapter 22, at the end of the 1980s, significant events led to the examination of the conditions under which equipment maintenance is organized and performed. Based on the 'Noc Report'[692], in particular, EDF took a certain number of steps that will be described in further detail in this chapter.

25.4.1. Management of a scheduled reactor outage for refuelling and maintenance

Reactor outages are scheduled to renew part of the nuclear fuel in the core and to carry out a large number of preventive and curative maintenance operations on equipment (see Chapter 26). It should be recalled that although maintenance activities

[690] Inspired by the human performance approach used in North America: self-checks, 'structured' communication, cross-checks, the 'one-minute pause', pre-job briefing and debriefing.

[691] Structured communication is mainly based on cross-checking communication between operators, which involves having the person who receives an order repeat and reformulate it back to the person who gave the order.

[692] See Section 22.2.1.

are performed throughout the year during reactor production, around 80% of them are completed during reactor outage. During reactor outage, maintenance operations are performed by several hundred EDF employees and its contractors.

In the 1990s, the search for improved cost control led EDF to reconsider the duration of scheduled outages at its reactors, which were much longer than those in other countries: how could the availability of the reactor fleet be improved without compromising safety or the quality of operations? EDF then worked to improve the manner in which scheduled reactor outages were prepared and organized by having facilities adopt the ‘project mode’ to organize outages from the mid-1990s onwards.

There are several phases to a scheduled reactor outage, as shown in Figure 25.2.

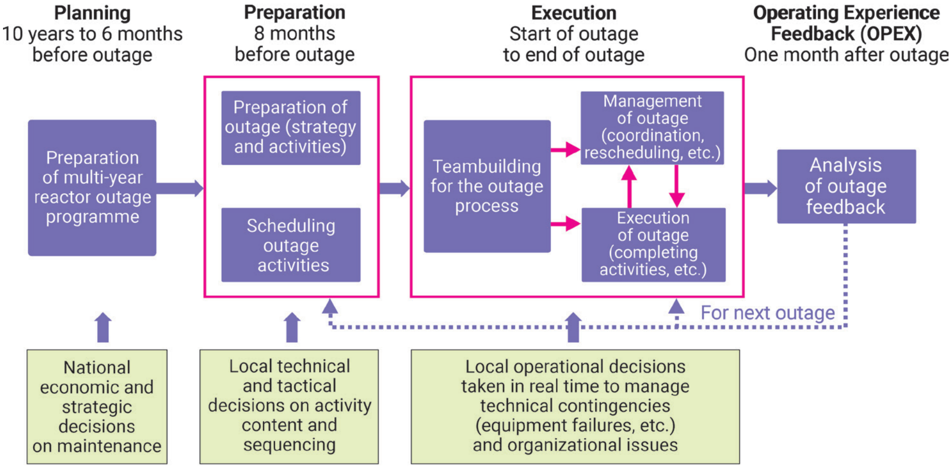

Planning
10 years to 6 months
before outage
Preparation
8 months
before outage
Execution
Start of outage
to end of outage
Operating Experience
Feedback (OPEX)
One month after outage
Preparation of multi-year reactor outage programme
Preparation of outage (strategy and activities)
Scheduling outage activities
Teambuilding for the outage process
Management of outage (coordination, rescheduling, etc.)
Execution of outage (completing activities, etc.)
Analysis of outage feedback
For next outage
National economic and strategic decisions on maintenance
Local technical and tactical decisions on activity content and sequencing
Local operational decisions taken in real time to manage technical contingencies (equipment failures, etc.) and organizational issues

Figure 25.2. The different phases of a scheduled reactor outage and the decision-making levels. IRSN.

The main phases of preparation, planning, execution and operating experience feedback are coordinated by about 50 personnel members from EDF. These personnel members are seconded from the maintenance and operations teams to form an ‘outage project team’ for several months, based in a dedicated building. From within this team, a management team of about 12 people is selected to manage the preparation and execution of the outage and collect operating experience feedback; this team has a dedicated room equipped with communications systems.

Later, in the 2010s, EDF set up a system for managing unit outages known as the ‘outage control centre’, described in Section 25.2.5.

25.4.2. Risks during reactor outages

Nuclear fuel must continue to be cooled while the reactor is shut down. During maintenance work, some safety-related equipment may become temporarily unavailable, meaning that appropriate compensatory measures are required. These maintenance operations may be the source of errors, despite the prevention and reliability improvement steps taken. Such errors can make a safety function less reliable and generate 'latent defects' that are only detected during requalification testing, or else when the equipment is first used again during electricity generation, or during a subsequent outage. Nearly half of all significant events occur during reactor outage phases[693]. In addition, 80% of the collective dose received annually by EDF employees and its suppliers is associated with maintenance operations performed during scheduled outages.

While the control of risks associated with maintenance operations depends on operational decisions taken in real time (for example, checking that safety postings and markings are suitable for the real-life conditions encountered), it also depends on decisions taken upstream regarding the conditions in which these operations are to be performed (for example, choosing operators according to their skills, equipment involved in the operations, etc.). In this respect, measures must be taken to ensure a good flow of information involving all relevant disciplines (operations, electrical systems and automatic control, mechanics, boiler work, etc.), including contractors.

25.4.3. Preparation for scheduled reactor outages

The scheduling of maintenance work by EDF's corporate services in liaison with facility management is carried out with the aim of anticipating workloads to adjust resources to the work to be performed. For certain major works, such as those associated with ten-yearly outages, scheduling begins ten years prior to the outage. Scheduling is also important in terms of visibility for suppliers, as it enables them to ensure that the right skills are available at the right time. For each scheduled outage, the detailed maintenance programme is defined by the outage project team, in agreement with corporate services, several months before the outage; this should give the workers involved time to prepare the thousands of operations required in good conditions. Work meetings are held to take into account the various aspects of each operation and the progress of preparations is regularly monitored within the project outage team. Operating experience feedback from previous operations is integrated at this stage.

The organizational measures decided by EDF for planning and preparing scheduled reactor outages should, in principle, ensure that maintenance operations are completed in a way that is compliant with safety and radiation protection requirements. However, in practice, after the detailed programme has been drawn up, outage preparation may be complicated by the addition of extra work to the maintenance schedule (for example, when premature ageing of equipment is discovered) or even due to the limited availability of personnel with certain specializations, who also have to respond to the demands of other reactors at the site. In 2013, following technical reviews conducted by IRSN and presented to the Advisory Committee for Reactors, ASN asked EDF to reinforce and 'protect' the conditions for preparing scheduled reactor

[693] Some of these are events significant in terms of radiation protection, as they occur when equipment undergoes radiographic inspection as part of non-destructive test programmes.

outages. As an example, EDF introduced additional measures to improve control over late work requests, which might be justifiable but which would overburden or even disrupt the preparation and execution of operations.

Lastly, EDF's desire to extend the operation of nuclear power plants beyond 40 years will lead to an increase in the volume of maintenance work. With this in mind, the balance between workloads and available resources must be maintained, ensuring that there are sufficient margins where necessary.

25.4.4. Managing scheduled reactor outages

Managing scheduled outages in project mode promotes the coordination of the various disciplines that are needed to perform more than one hundred operations each day, while also handling any unexpected issues that may arise during maintenance operations. These issues may be organizational (for example, the unexpected unavailability of suitably qualified personnel or the temporary unavailability of spare parts) or equipment-related (for example, the need to replace a valve found to be defective during checks). For the outage management team, these issues must be resolved in real time, as far as possible without extending the outage time; this can, however, be detrimental to the preparation of activities to be performed on subsequent days.

Despite the fact that the outage schedule is drawn up in advance to organize the activities of the various parties involved, their coordination remains a constant concern. Regular schedule updates can lead to changes in the planning of operations, which may affect how well operators can coordinate with one other.

Making sure that the management team for a scheduled outage includes representatives from different disciplines and personnel with recognized expertise in nuclear safety and radiation protection has structurally improved the way in which the various issues are taken into account during the necessary trade-offs to be made during an outage. However, achieving good team performance requires being attentive to the concerns expressed by the different participants. In some specific situations, the exercise of responsibilities or the status of personnel with particular expertise can lead to divergent views likely to result in inappropriate trade-offs (for example, to the detriment of radiation protection requirements when operating scenarios are adjusted).

Cutting corners when sharing information and making decisions in order to increase efficiency can mean failing to call upon sources of expertise or managers as planned, threatening the structure established to ensure effective risk control.

25.5. Supervising outsourced activities

As seen above, most maintenance operations performed during scheduled reactor outages have been outsourced by EDF since the 1990s. In certain areas (for example, valve maintenance), up to 80% of maintenance operations are outsourced. Sites with two reactors can therefore see their population double during these outages. Nevertheless, EDF still has to fully exercise its responsibility in terms of nuclear safety, which means ensuring that the right skills are available internally, in terms of both technical expertise for work execution and supervision skills to oversee contractors.

Since the 1990s, this issue has been the subject of regular discussions between EDF and safety organizations. In the first instance, it was considered in relation to the way in which EDF monitors the quality of work performed by contractors, in application of the Quality Order of 10 August 1984. In light of the analyses performed by IPSN, then IRSN, as well as observations made by the inspectors of basic nuclear installations during oversight inspections, the discussions were then broadened to cover all contracting processes. At the request of ASN, in 2013 and 2014 IRSN undertook an in-depth analysis of all stages of the contracting process: qualification of companies, contracting, planning, preparation, execution of operations, evaluation of services and operation, as well as operating experience feedback from outsourced activities.

During this analysis, contracting was addressed from the perspective of the contractual relationship that binds the project owner to the contractors, and its influence on how safety issues are incorporated into maintenance operations. Certain matters arising from this analysis are developed further below.

25.5.1. Contractor qualification and contracting

To ensure that contractors have the necessary capacity to perform operations likely to have an impact on safety, the first stage of the process developed by EDF is to qualify these companies before signing a contract with them. This qualification stage allows EDF to check that the companies in question have the management provisions (quality and risk management system, skill and certification management system, etc.) considered necessary to perform activities while meeting the required level of safety and quality, and to exclude companies that do not meet these conditions, especially during the tendering process. The qualification process must also give the facility operator the ability to evaluate the actual performance of the management provisions of the companies concerned. In this respect, EDF has a qualification process that depends on the completion of work performed under surveillance (‘conditional qualification’).

The contracting process also aims to give contractors visibility over their workload in the medium term, allowing them ample time to recruit and train their teams. EDF’s introduction of national multi-year contracts for repeated activities of significant volume has been recognized as an example of best practice.

25.5.2. Matching workload and resources

The preparation and management of maintenance services aims to guarantee and maintain an adequate balance between workload and the competent workforce available. In this respect, when planning a scheduled outage it is important to take into account contingencies and their consequences, particularly in terms of how the workload is adjusted to both internal resources (operation, automatic control, maintenance, etc.) and external resources (contractors). The schedule is discussed and adjusted many times by the outage management team, the different disciplines involved and contractors.

During the outage itself, the schedule is updated on a daily basis by incorporating the actual progress made, any delays encountered or predictable and – where necessary – new operations required, so as to re-establish a balance between the workload and competent personnel available. This means that EDF and its contractors must remain capable of accepting a certain amount of flexibility (by allowing amendments to initial contracts, late orders, etc.). Compensatory mechanisms do exist (such as payment for hours on standby, or early breaks for a team so that they can return at night, for example), but it can be difficult to make adjustments in real time. As a result, contractors' capacity to adapt and react requires strong commitment from the employees involved. Furthermore, to counteract the potential negative effects of these adjustments, for example the urgent reassignment of an operation to operators who were not involved in preparing it, or who are less skilled or experienced than the operators initially assigned, it is important to ensure that any risk analysis arising from adjustments is duly shared with the contractor(s) concerned.

25.5.3. Carrying out work

The reliability of maintenance operations depends on a wide range of measures implemented from the preparation phase, during drafting of the operation schedules and the maintenance documentation, which includes procedures, operating instructions and risk analyses (see Section 25.2.3.). As close as possible to the operation, a preliminary meeting is held to check that the prerequisites have been met, i.e. that all the conditions for the operation are indeed in place (spare parts are available, signage has been put up at the work site, etc.). These preliminary meetings constitute best practice for improving the reliability of operations and limiting contingencies. During IRSN analyses conducted in 2013 and 2014, it did however become clear that, in the event of contingencies or where prerequisites were not met, a more formal method was needed to handle any exemptions made.

Since 2011, EDF has implemented new measures to reduce the time needed for operations by shortening 'hands-on' time[694]. These new measures involve ensuring that contractors are more closely involved in preparing activities, reinforcing the field presence of internal supervisors for contractors, increasing logistic support for operation managers and introducing 'one-stop shops' for logistic support[695]. Given that they make it easier to meet the prerequisites for operations and reduce the workload of the operating crews, these measures should have a favourable effect on safety; EDF will evaluate their effectiveness over the long term.

[694] For operators, 'hands-on' time is the time spent actually working on an equipment item. The improvement goal of EDF is to make sure that operators can focus on their operation without wasting time on travelling or waiting to get tools or work permits.

[695] Points where all logistic functions required for operations are grouped together – one for controlled areas, the other for non-controlled areas.

25.5.4. Surveillance of outsourced activities

As indicated above, to exercise its responsibilities as a facility operator, EDF must oversee the activities performed by its contractors and suppliers. Regulatory requirements in this respect were historically set out in the Quality Order of 10 August 1984, before being reworked and expanded in the INB Order of 7 February 2012 (supplemented by Decree 2016-846 of 28 June 2016).

Under these regulatory requirements, any activity important for 'protected interests' that is entrusted to an outside operator must be overseen. Surveillance must allow the facility operator to ensure that personnel complies fully with the stipulated requirements regarding activities and items important for protected interests that are associated with operations (for example, the tightening torque for a flange), and correctly apply the facility safety policy. Surveillance actions must be proportionate to the risks associated with the operations. In addition, the human resources allocated to surveillance must be adequate in terms of number and skills in order to correctly determine which surveillance actions must be carried out, then implement them and draw on lessons learned as part of continuous improvement.

EDF has long-standing measures, reinforced in recent years (2013 and 2014), that aim to improve the reliability of contractor surveillance: an established surveillance policy, a surveillance management guide with quantitative references for 'sizing' the corresponding workforce, task descriptions and guidelines on renewing technical skills for surveillance managers, etc. Safety organizations have observed, however, that improvement is slow and problems persist, as seen regularly during surveillance inspections. Furthermore, the Major Refit programme will entail greater surveillance needs. It is important to assess the effectiveness of improvements over the long term. ASN has asked EDF to go beyond occasional observations or general indicators that are too broad and implement operational indicators to measure the effectiveness of surveillance.

25.5.5. Operating experience feedback and assessing outsourced activities

As part of its contractual approach, EDF completes an evaluation at the end of each delivered service in order to record the quality of that service and any deviations encountered. From a risk-control perspective, it is important to take measures to capitalize on the operating experience feedback from the hundreds of thousands of maintenance operations that are performed every year by contractors across the entire nuclear power plant fleet. Lessons learned should be used to assess and improve the measures taken to effectively manage outsourced activities. Systematic analysis of operating experience, taking into account the characteristics of the work accomplished and its conditions of performance, should identify the causes of any difficulties, failures or malfunctions – whether organizational or contractual – that occur during operations, whether they originate with EDF or the contractors.

However, the wide variety of channels for reporting information on operations, services and contractor activities complicates the processing of feedback, especially in terms of cross-cutting statistical analysis (between several contractors, several sites, etc.) when attempting to identify trends. This is why EDF has introduced new tools since 2016, consisting of more comprehensive databases and new service evaluation sheets, aiming to highlight service performance factors for both the contractor and EDF.

Despite the asymmetric relationship between the 'user', EDF, and any contractor, it is generally recognized that assessing a service is not solely a matter of considering the contractor's contribution, as the user can also show organizational weaknesses or inadequacies (for example, by failing to ensure that prerequisites for operations are met). It is therefore essential for the facility operator to transcend the traditional customer-supplier contractual relationship and favour an approach that considers the completion of a service to be the result of a joint contribution by the user and the contractor. This shift in approach is a necessary condition for achieving better control of outsourced operations.

It should also be noted that ASN carries out annual inspections of outsourced maintenance operations during unit outages. In addition, in 2018 it inspected all sites on the basis of a guide drawn up by IRSN using the conclusions of the analyses performed in 2013 and 2014.

Lastly, as stated in Chapter 4, within the Steering Committee for Human, Social and Organizational Factors created following the Fukushima Daiichi nuclear power plant accident, there is a working group that examines outsourcing issues in maintenance; this group met with all basic nuclear installation operators between 2013 and 2016. A report formalizing these discussions is available on the ASN website[696].

[696] Report entitled *Pour une contribution positive de la maintenance sous-traitée à la sûreté nucléaire* (For a Positive Contribution of Outsourced Maintenance to Nuclear Safety), available at https://www.asn.fr/L-ASN/Comite-sur-les-facteurs-sociaux-organisationnels-et-humains.

Chapter 26
Facility Maintenance

Proper implementation of defence in depth, which requires detection of anomalies and deviations relative to normal operating domains, entails – in addition to monitoring operating parameters and conducting periodic testing – performing preventive maintenance and monitoring equipment important to safety in order to avoid their failure, as far as possible, as well as taking appropriate action to remedy any observed anomalies and deviations (corrective maintenance). This chapter describes the various aspects of maintenance.

Chapter 27 addresses actual in-service monitoring, illustrated by applications to certain major items of reactor equipment in the nuclear power fleet.

26.1. Maintenance objectives

The maintenance objectives for a nuclear facility such as a power-generating reactor are to maintain equipment performance levels and reliability throughout its service life, including aspects related to nuclear safety, with special consideration given to maintaining the qualification of equipment likely to be used in incidents or accidents. In order to achieve these objectives for the entire nuclear power plant fleet throughout reactor lifetime, Électricité de France (EDF) must anticipate and address a wide variety of constraints, such as component obsolescence or ageing, a changing industrial base and technological developments, together with changes to maintenance baselines and regulatory requirements, staff turnover and, of course, economic constraints.

The reactors in the nuclear power fleet do not all have the same age and incorporate different technologies, in particular with regard to control rooms and the instrumentation and control system. EDF therefore must therefore manage a major and variable ‘volume’ of maintenance operations involving numerous items of equipment and different fields and technologies, which may or may not be important to safety.

These industrial circumstances have an impact on the planning of unit outages, which is when most preventive maintenance is carried out, in order to ensure availability of the necessary human, technical and logistical resources.

However, while essential, maintenance may also be a source of errors and malfunctions. In the late 1980s, a number of events caused by maintenance operations highlighted the important impact of maintenance performance on safety. Some of these events are mentioned in the chapters dedicated to operating experience feedback, which explain that, at the request of public authorities, EDF undertook a critical analysis of maintenance quality in 1989. This analysis led to major transformations within EDF, in particular by introducing fundamental changes such as the ‘maintenance initiative’ and subsequently the ‘maintenance safety initiative’.

The remainder of this chapter describes the general principles of nuclear power reactor maintenance and the various associated strategies implemented by EDF and explains the conditions for successfully carrying out maintenance at facilities, providing illustrative examples of certain problems encountered.

26.2. Maintenance

26.2.1. Definition

Maintenance is “the combination of all technical, administrative and managerial actions taken during the life cycle of an item in order to maintain or restore a state in which the item can perform the required function” (French standard NF EN 13306).

Generally, maintenance within an industrial facility involves selecting maintenance methods, developing and optimizing maintenance programmes, partially or completely outsourcing maintenance tasks, requalifying the equipment, managing spare parts and logistics, training maintenance personnel, considering the economic impact, etc.

There are several different types of maintenance, as shown in Figure 26.1.

Preventive maintenance includes those actions taken to reduce the probability of failure or deterioration of an item of equipment; maintenance is systematic when it is carried out according to a fixed schedule or on the basis of a number of units of use (such as a number of motor starts), regardless of the state of the equipment, and is conditional if it is carried out only when it shows a significant state of degradation defined by a predetermined threshold.

Corrective maintenance includes those actions taken after the failure of an item of equipment in order to restore it to a state in which it is capable of performing its function; it is referred to as ‘temporary’ when this operation is provisional (troubleshooting) and is ‘curative’ when the operation is permanent (repair, replacement).

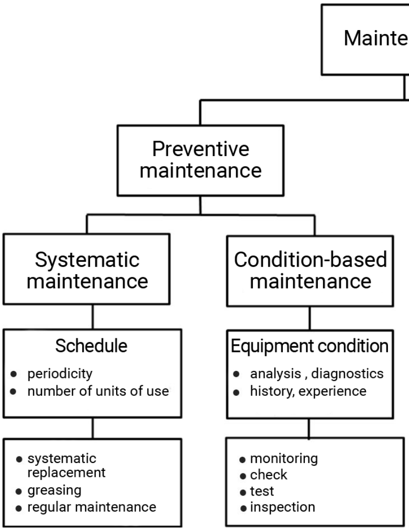


Figure 26.1. The different types of maintenance. IRSN.

26.2.2. Maintenance strategies

Facility equipment is subject to deterioration mechanisms which may lead to failure modes[697], thus bringing about partial or total unavailability. These deterioration mechanisms may be of a technical nature (wear, fatigue, ageing, corrosion, etc.), or arise from human and organizational factors (error, omission, improper use, etc.).

The kinetics of deterioration mechanisms depend mainly on equipment operating conditions (numerous starts and stops, continuous operation, etc.), environmental conditions (humidity, salinity, etc.) and scheduled maintenance tasks.

Given the many kinds of equipment present in a nuclear power reactor, EDF has developed maintenance strategies in order to ensure the level of reliability required on the different types of equipment.

Accordingly, since 1994, using operating experience feedback and probabilistic safety assessments as a reference, it has implemented systematic preventive maintenance for systems of major importance in terms of safety, availability, radiation protection and cost. This preventive maintenance programme was defined on the basis of a reliability-centred maintenance optimization process.

This type of maintenance strategy frequently involves regular and planned withdrawal of equipment from service in order to carry out an intrusive maintenance task.

[697] Failure modes describe the malfunctioning of an item of equipment which no longer fulfils its function. Five generic failure modes may be identified: loss of function, untimely operation, refusal to stop, refusal to start and degraded operation.

Furthermore, in the early 2000s, EDF also began to develop and use conditional maintenance, based particularly on monitoring 'reference equipment items'. This strategy makes it possible to limit not only the number of intrusive activities, but also exposure to ionizing radiation for the personnel involved. EDF does not intervene on all the relevant equipment items until signs of deterioration that might jeopardize equipment performance levels are identified on the reference equipment items.

26.3. Optimizing maintenance

Maintenance optimization procedures include risk analysis and operating experience analysis to ensure the appropriate maintenance tasks are selected. From this perspective and, as mentioned above, EDF has developed a Reliability-Centred Maintenance (RCM) optimization method.

26.3.1. Reliability-centred maintenance

The RCM method developed by EDF is a general method for optimizing equipment maintenance choices that depends on to what degree the failure modes of an equipment item contribute to operational performance, taking into consideration the impact in terms of cost and reliability.

The first-generation RCM method was developed in the 1990s by EDF research and development units and was based on methods developed for aeronautic and military applications in the USA, then adapted to nuclear applications by the Electric Power Research Institute (EPRI).

The factors selected by EDF when conceiving the first generation of RCM methods were safety (including compliance with operational limits and conditions and contribution to the risk of accidents with core melt), availability of systems important to safety, and maintenance costs.

The method is based on a functional system approach, no longer the equipment approach. It takes into account the consequences of failure at system or facility level.

An RCM study includes five phases (see Figure 26.2).

The first phase involves describing the system under examination in functional terms and analysing its failure modes and their effects (FMEA). This enables precise identification of the functional and physical limits of the analysed system and divides the facility into functional groups (FG). The effects of each failure mode of a functional group are then analysed and their severity is evaluated in terms of safety, availability and maintenance costs, according to a predefined matrix.

The second phase involves finding failures inside the functional group that are capable of bringing about failure modes considered as severe during the first phase and then evaluating the 'criticality' of these failures (FMECA phase). This is accomplished by dividing the functional groups into technological assemblies and, if necessary, into technological subassemblies and components, according to the item actually requiring the relevant maintenance operations. The causes of failures on the technological assembly or technological subassembly are then analysed to identify those which lead to any failure mode considered as severe during the previous phase. The 'criticality' of these failures is then evaluated using criticality thresholds based on operating experience feedback.

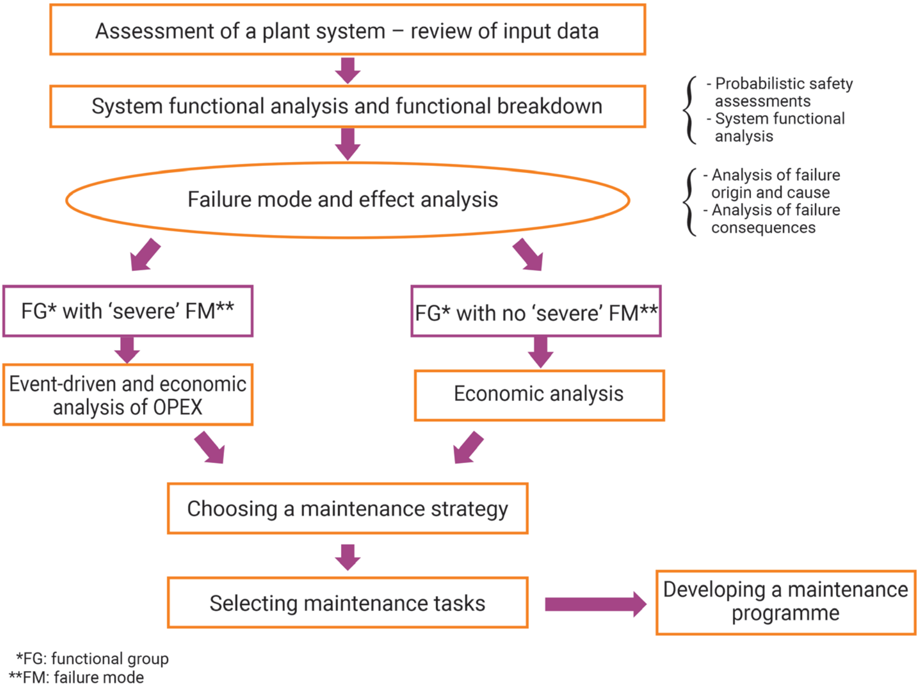

Assessment of a plant system – review of input data
System functional analysis and functional breakdown
- Probabilistic safety assessments
- System functional analysis
Failure mode and effect analysis
- Analysis of failure origin and cause
- Analysis of failure consequences
FG* with 'severe' FM**
FG* with no 'severe' FM**
Event-driven and economic analysis of OPEX
Economic analysis
Choosing a maintenance strategy
Selecting maintenance tasks
Developing a maintenance programme
*FG: functional group
**FM: failure mode

Figure 26.2. Diagram of RCM steps. IRSN.

The third phase is an event-driven and economic analysis of lessons learned which actually proceeds in parallel with the second phase because the data generated are used in the second phase.

The fourth phase involves determining the maintenance 'strategy' and selecting maintenance tasks that are appropriate with regard to the faults to be avoided. A maintenance strategy for establishing or changing an existing maintenance programme is selected on the basis of 'critical' failures, their level of severity, performance factors derived from operating experience feedback and the presence or absence of a preventive maintenance programme. A preventive maintenance task is thus systematically defined for each 'critical' failure identified during the second phase.

The fifth phase involves writing the basic preventive maintenance programme by grouping maintenance tasks together at the functional group level in order to obtain an overview of all the selected tasks. When identical tasks are applied to an item of equipment for different failure modes, they are, of course, carried out just once. When periodicity differs, a new value common to each of the modes concerned is defined. The final maintenance choice is essentially based on expert opinion and optimization of the costs and feasibility of the selected maintenance tasks.

This first-generation RCM method was implemented between 1994 and 2001. It resulted in 150 'RCM programmes' covering over 50 elementary plant systems on 900 MWe units in the CPY programme contract and on 1300 MWe reactors. Operating experience feedback from these years of application led EDF to consider that, while the method's results were satisfactory with regard to the initial objectives, it was difficult and heavy in terms of implementation. More widespread use of RCM meant that changes in the method would be necessary.

EDF therefore decided to implement a 'second-generation' RCM method for developing RCM programmes, especially for the 900 MWe units in the CP0 group and the 1450 MWe units in the N4 series, with regard to the systems of major importance selected when the first-generation method was applied.

The second-generation RCM method adopts the main principles of the first-generation method. The main change is the elimination of the FMECA phase, and hence of the notion of 'criticality', because EDF found it to be very 'costly' in terms of study time and maintenance. 'Criticality' was the expression of the result obtained when severity and frequency were paired together for a given failure mode. Considering a technological assembly to be 'critical' for a given failure mode systematically meant that it was necessary to define a preventive maintenance task. The second-generation RCM method has incorporated other changes, such as taking into account personnel safety and environmental risks.

The viewpoint of safety organizations is that the (second-generation) RCM method (still in force) should be used with caution because:

- there is a risk this method will lead to a considerable reduction in preventive maintenance operations, while a large portion of maintenance operations must be carried out on a random basis in order to increase the chance of detecting new or unpredicted deterioration phenomena at an early stage;
- failure rates, which are of great importance for the method, are generally marked by significant uncertainty.

It has, however, been possible to take these reservations into account in complementary investigation programmes, which will be addressed below (see Section 26.5.2) and in Chapter 30 on periodic reviews.

26.3.2. Conditional maintenance

Conditional maintenance is a preventive maintenance strategy based on monitoring the operation or important parameters of an equipment item. EDF uses this approach to avoid carrying out systematic preventive maintenance of an intrusive nature.

A conditional maintenance study comprises six steps:

1. preliminary analysis,
2. functional analysis and failure mode analysis (FMEA),
3. analysis of operating experience and identification of failure detection means,
4. defining instruments required for monitoring (types of sensors, etc.),
5. selection of maintenance tasks,
6. technical and economic analysis.

Once the study has been validated, the corresponding conditional maintenance tasks are incorporated into the maintenance programme for the equipment in question. Implementation of a conditional maintenance programme therefore involves in-service monitoring of the state of the relevant equipment item, and conducting a technical analysis of the resulting data to determine if and when intrusive inspection is necessary. This is accomplished by:

- monitoring the relevant equipment, which requires good knowledge of equipment deterioration modes, the faults likely to occur and providing the measuring instrumentation required for monitoring;
- detecting any symptoms that may indicate the onset of deterioration. This can be accomplished by monitoring parameter deviations or even, in some cases, specific thresholds;
- conducting diagnostics, again, based on monitoring parameter changes;
- forecasting, which requires good knowledge of deterioration modes and the availability of operating experience feedback. This phase serves to track the kinetics of detected deterioration based on monitoring and knowing which parameters impact deterioration. This makes it possible to estimate the time to a possible failure;
- taking maintenance decisions, which must be done by the responsible authorities because they involve a certain degree of risk with regard to availability and cost (increase in monitoring periodicity, decision to stop or postpone a maintenance operation).

The difficulty of introducing this method resides in deciding which parameters will be monitored and determining with certainty that they will be capable of detecting any equipment deterioration likely to lead to failure.

The detection, diagnostics and forecasting phases presented above are based on follow-up of parameter deviations acquired during the monitoring phase.

26.3.3. Conditional maintenance by sampling – Maintenance based on reference equipment items

The assumption behind this maintenance philosophy is that it is possible, under certain conditions, to identify items of equipment that are representative of an entire set of equipment in terms of their state of wear, and therefore in-depth testing and inspection may be limited to these 'reference equipment items'.

The maintenance method based on reference equipment items therefore involves, for a given family of equipment, carrying out a preventive maintenance programme comprising a 'complete inspection'[698] of a limited selection of equipment items, while applying a simplified maintenance programme to the remaining items in the equipment family.

This method generally involves equipment that is subject to a preventive maintenance programme for which operating experience has revealed no (or little) deterioration or failure following preventive maintenance operations. It may involve both active equipment items (in particular valves, rotating machines, electrical equipment) and passive equipment items (such as the stationary parts of electrical switchboards).

This approach mainly targets items that are not subjected to large loads, and, in particular, equipment that is monitored through periodic testing.

A maintenance study based on reference equipment items comprises five steps:

1. preliminary analysis to: identify all documents that may be pertinent to the study, characterize the technical equipment family, and define the scope of the study,
2. functional analysis and failure mode analysis (FMEA),
3. choosing the maintenance strategy,
4. selecting maintenance tasks,
5. writing the maintenance programme.

The sensitive point of this strategy is selecting a sample of reference equipment items from a 'technical family' of homogeneous equipment items. The study must therefore begin by analysing the level of equipment homogeneity based on the following criteria:

- technological data (type of equipment, technology, component materials, fluids conveyed, sizing characteristics),
- operating conditions (continuous or standby operation, etc.),
- environmental conditions (operation indoors, outdoors, coastal location, etc.).

[698] An operation involving disassembling a certain number of components on the equipment item in question so that it can be thoroughly inspected.

If a ‘technical family’ is not homogeneous, the items of equipment are classified into subfamilies. A ‘technical family’ of equipment is then made up of several subfamilies of homogeneous equipment.

The reference equipment items must be the first items of equipment that may be subject to deterioration or failure, so that action can be taken on the other items of equipment in the family before they show signs of deterioration or failure.

Thus, after identifying the failure modes covered by a complete inspection of the reference equipment items, i.e. the failure modes corrected by maintenance work carried out during the inspection, and the deterioration mechanisms underlying these failure modes, two additional processes known as ‘proactive’ reasoning and ‘‘retroactive’ reasoning are applied to identify the most degraded equipment. Proactive reasoning determines which factors have an impact on deterioration mechanisms and identifies which equipment items are the most exposed to these factors. Based on operating experience feedback, retroactive reasoning determines which equipment items are the most susceptible to the relevant deterioration mechanisms. Applied alone, neither type of reasoning is capable of covering all the deterioration mechanisms that can affect the reference equipment item, because there is not enough data or ‘before-the-fact’ knowledge available. According to EDF, a combination of both types of reasoning can provide answers and compensate for any lack of data in one or the other type of reasoning.

Another method is also used for selecting reference equipment items. This is the statistical method, which is only appropriate for a large equipment family (consisting of several hundred items) and when there is no single characteristic that can be used to determine which items are the most degraded. For this purpose, EDF has a numerical tool that uses the formulas in French standard NF X06-068 (on estimating a proportion). This tool is used to establish the number of reference equipment items required to state, within a given confidence threshold, that the difference between the proportion of degraded items in the entire equipment family and the proportion of degraded items in the sample of reference equipment items is below a given accuracy threshold.

If an unforeseen event occurs in an equipment family, it must be analysed to establish the source of the fault, whether or not it is generic and the urgency of any action to be taken. These actions may result in an increase in sample size, a return to systematic inspection or a change in inspection periodicity.

Following discussions with IRSN, EDF has agreed to carry out complete inspections of every item in an equipment family, and not just the reference equipment items, but with a frequency that is less than that applicable to the reference equipment items.

26.3.4. ‘AP-913’ method

Despite the contributions made by the Reliability-Centred Maintenance method, certain limitations have been identified. More specifically, RCM studies, which are still conducted, most frequently:

- lead to a change in the frequency of preventive maintenance tasks, but rarely to a change in the type of tasks performed,
- introduce relatively few conditional maintenance tasks (except in the case of rotating machines).

However, for EDF the use of conditional maintenance is a major pillar of its maintenance strategy, which aims to limit the number of maintenance operations carried out on equipment and, more specifically, those tasks entailing outages and intrusive inspections.

Studies on equipment and the associated maintenance needs are conducted for this purpose. Equipment health is analysed to define maintenance analysis 'thresholds' based on the condition and behaviour of equipment.

A study on reference equipment items serves to reduce the volume of maintenance by inspecting only a limited sample of items.

In order to capitalize on the various contributions made by the strategies set out above, in 2008 EDF decided to implement the AP-913 (Advanced Project 913) method defined by the Institute of Nuclear Power Operations (INPO).

The aim of this method, developed by INPO starting in 2001, is to improve the reliability of equipment important to safety, along with facility availability. This method is based on an analysis of equipment behaviour and operating conditions in order to adapt the maintenance and monitoring efforts applied to each equipment item according to the potential consequences that failure of this item would have on safety and reactor availability (which defines equipment 'criticality').

With this new method, EDF aimed to boost fleet availability to a rate of approximately 85%.

The AP-913 method comprises six points:

1. identification of 'critical' equipment in facilities, specifying the functions and performance of each equipment item and characterization of the item's contribution to safety, power generation, environmental protection, etc.,
2. applying in-service monitoring to the equipment item, accompanied by analysis and understanding of the deterioration mechanisms at work and identification of relevant predictive indicators,
3. defining corrective action to be applied to equipment, specifying the causes of observed failures, the conditions in which they are initiated and develop, and conceivable improvements,
4. implementing continuous improvement of equipment reliability, including the creation of a 'follow-up and maintenance framework',
5. defining long-term management of equipment life cycles and maintenance programmes with periodic evaluation of equipment health, follow-up and

prediction of the progression of ageing mechanisms, detection of obsolescence and introduction of long-term strategies to control it,

6. implementation of preventive maintenance and organization of scheduled maintenance tasks.

AP-913 examines a certain number of areas already covered by RCM and conditional maintenance methods. It does, however, result in a specific organization of maintenance services and complementary actions, such as:

– the definition and systematic use of performance indicators (both for equipment and organizations),

– a short loop for operating experience feedback and modifying maintenance programmes.

Safety organizations have, however, notified EDF of several points requiring special attention with regard to the AP-913 method:

– first, the method involves introducing a process to leverage maintenance-related operating experience which, in addition to equipment monitoring, must allow maintenance efficiency to be evaluated; this entails appropriate organization, resources and tools;

– certain steps in the application of the method are fundamental and must be managed with special care (definition and development of follow-up criteria and performance indicators, representativeness of equipment health reviews, etc.);

– with regard to conditional maintenance based on reference equipment items, it remains important, for the purposes of defence in depth, to carry out equipment inspections based on sampling for those items where failure is considered to be a serious threat to safety as defined in the RCM method, and for which only corrective maintenance has been planned, regardless of how the AP-913 method classifies the equipment.

A new version of the AP-913 method is under development at EDF.

26.4. Maintenance baselines

To take into account the various requirements involving not only safety and regulations, but also equipment availability, the numerous ‘baseline’ sources pertaining to maintenance have become more substantial throughout the course of facility operation and the development of various strategies (see Figure 26.3).

With regard to maintenance, a general distinction is made between:

– the external baseline, consisting of regulations (the ‘regulatory baseline’),

– internal baselines established by EDF, namely the national baseline and ‘local’ baselines established at the facility level.

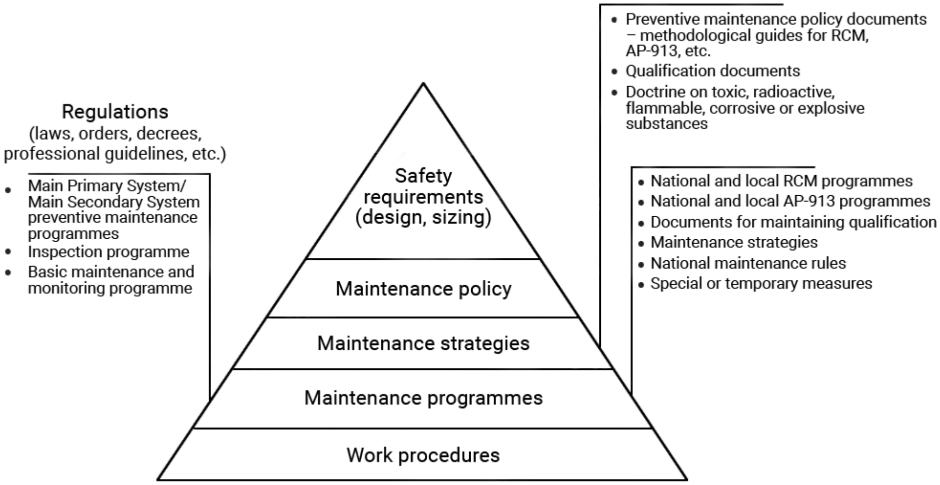

Regulations
(laws, orders, decrees, professional guidelines, etc.)
• Main Primary System/ Main Secondary System preventive maintenance programmes
• Inspection programme
• Basic maintenance and monitoring programme
Safety requirements (design, sizing)
Maintenance policy
Maintenance strategies
Maintenance programmes
Work procedures
• Preventive maintenance policy documents – methodological guides for RCM, AP-913, etc.
• Qualification documents
• Doctrine on toxic, radioactive, flammable, corrosive or explosive substances
• National and local RCM programmes
• National and local AP-913 programmes
• Documents for maintaining qualification
• Maintenance strategies
• National maintenance rules
• Special or temporary measures

Figure 26.3. The Maintenance Baseline documentation pyramid. IRSN.

Regulations require the facility operator to carry out a certain number of tests and inspections, primarily pertaining to the monitoring of pressure equipment[699]. The documentation corresponding to these regulations is subject to approval by the French Nuclear Safety Authority (ASN); this documentation cannot be modified, even provisionally, without prior agreement from ASN.

General principles are furthermore set out in certain texts relevant to maintenance[700], but that do not define specific maintenance tasks. The facility operator must establish which maintenance tasks are capable of observing these principles.

For items of equipment that are not subject to these texts, corporate services at EDF determine which items must be covered by national maintenance programmes for reasons of safety, availability, radiation protection or cost.

Studies conducted according to the methods described in previous sections serve as a basis for preparing national maintenance programmes. Supplements are added to these programmes to take into account equipment containing toxic, radioactive, inflammable, corrosive or explosive fluids (liquid or gaseous).

[699] Decree 99-1046 of 13 December 1999 regarding pressure equipment. Order of 10 November 1999 relevant to monitoring the operation of the main primary system and main secondary system on pressurized water reactors. Order of 12 December 2005 regarding nuclear pressure equipment (the ‘Pressure Equipment Order’).

[700] Order of 31 December 1999 stipulating the general technical regulations for preventing and limiting the detrimental effects and external hazards resulting from the operation of basic nuclear installations (repealed). Order of 1 March 2004 relating to the inspection of lifting equipment and accessories.

Requirements pertaining to equipment qualification for accident conditions are also taken into account for the purposes of developing maintenance programmes. Qualifying equipment for accident conditions and maintaining this status over the long term are key to ensuring the safety of nuclear facilities.

This set of maintenance programmes together with the various work procedures are part of the (national and local) maintenance baselines used within EDF. Modification of the programme does not require prior authorization by ASN. However, there is a system of internal exemptions in place whereby equipment experts are called in for cases of non-compliance with programmes (modification of the content of a task, non-compliance with task periodicity).

Operating documentation has seen considerable improvement since the first reactors of the French nuclear power fleet were commissioned. Taking into account operating experience has led to more precise descriptions of operating conditions. Furthermore, new operating requirements have gradually been introduced by EDF, not only to improve safety and protect workers and the environment, but also to boost the economic performance of facilities.

Since 2007, EDF has been rolling out a project to harmonize practices and methods in order to standardize operational documents and bring them closer to user needs. In order to achieve this goal, EDF has decided to gradually replace site-specific operational documents with standardized operating procedures common to all sites equipped with the same reactors. Site-specific details do, however, remain the responsibility of the site in question.

This project is supported by using the AP-913 method, which includes the definition of a ‘follow-up and maintenance framework’ for components belonging to the same ‘technical family’, and also the new Nuclear Technical Information System for nuclear facilities.

The new regulatory framework[701] means that there will be changes to the general operating rules, which will include a chapter entirely dedicated to maintenance. The outline of this chapter and the associated maintenance baseline have been defined. The documents approved by ASN together with their content should see further development depending on the regulatory status of the chapter devoted to maintenance. A chapter in the general operating rules devoted to maintenance has been planned for the Flamanville 3 EPR.

[701] Act 2006-686 of 13 June 2006 concerning nuclear transparency and safety (the ‘TSN Act’). Decree 2007-1557 of 2 November 2007 on basic nuclear installations and the control of the transport of radioactive substances as regards nuclear safety. Order of 7 February 2012 setting general rules for basic nuclear installations.

26.5. On-site maintenance

26.5.1. The various stages of maintenance operations

Figure 26.4 describes the various stages of a maintenance operation.

Each facility must apply the national maintenance baseline and adapt it to local circumstances, implement the various maintenance programmes and take into account maintenance experience feedback produced not only locally, but also on a nationwide scale.

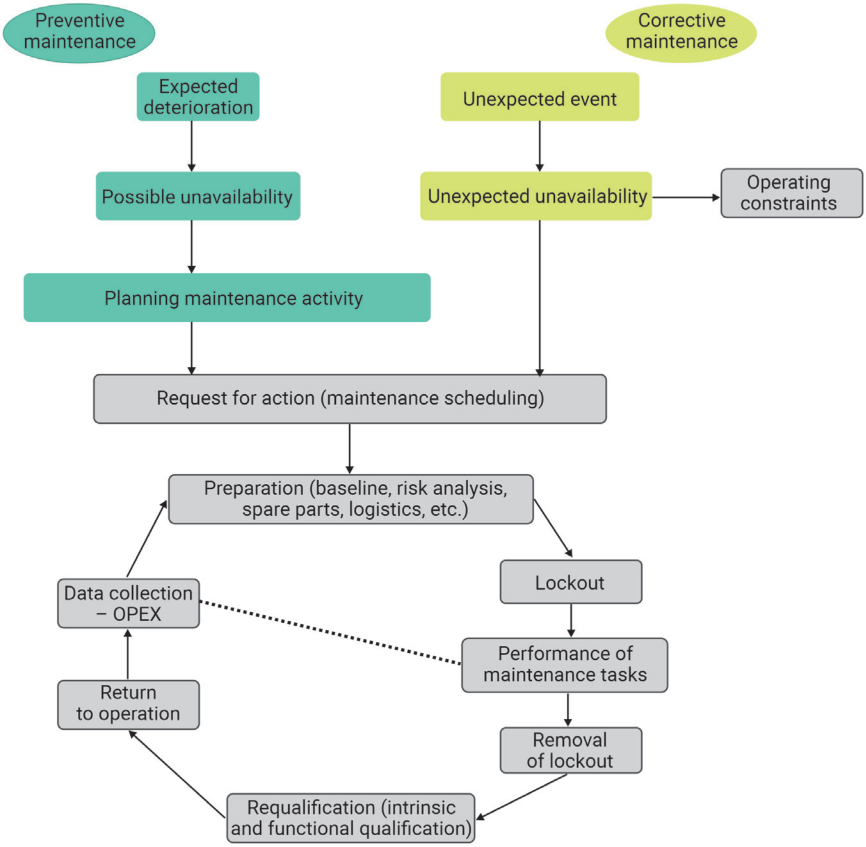

Preventive maintenance
Corrective maintenance
Expected deterioration
Unexpected event
Possible unavailability
Unexpected unavailability
Operating constraints
Planning maintenance activity
Request for action (maintenance scheduling)
Preparation (baseline, risk analysis, spare parts, logistics, etc.)
Lockout
Data collection – OPEX
Performance of maintenance tasks
Return to operation
Removal of lockout
Requalification (intrinsic and functional qualification)

Figure 26.4. Stages in maintenance work. IRSN.

Carrying out maintenance task(s) on an equipment item requires preparation to ensure that the work can be carried out under conditions that are safe for both the facility and workers. This preparation first involves identifying and collecting:

– documents required to carry out the various tasks ('lockout' – see definition below –, site logistics, safety procedures, hold points and checks, work procedures, requalification, etc.),

- documents specifying the required resources (tools, spare parts, number of persons required and their qualifications, outside services, required maintenance time, etc.).

The important steps in preparation are:

- risk analysis: this analysis is necessary before any maintenance operation in order to identify all risks associated with the operation and establish the necessary countermeasures. These risks may be related directly to the operation, but may also be related to the environment in which the work is to take place;
- predictive assessment of radiation doses related to the maintenance work;
- definition and provision of the associated logistics (spare parts, tools, utilities, packing materials, radiation protection, protection from fire or explosion risks, etc.);
- allocation of tasks among the various specializations required to conduct the maintenance work;
- definition and provision of human resources (personnel qualification).

All the operating documents relating to equipment ‘lockout’ are prepared during the preparation phase, since lockout is an integral part of the maintenance operation. The purpose of lockout is to allow personnel to work in completely safe conditions by preventing any possibility of inadvertent supply of utility fluids (electricity, water or other fluids) to the equipment being serviced.

Once the work has been completed, requalification must be performed. This is an important step carried out to ensure that equipment or system performance has not been degraded. Requalification comprises two parts: intrinsic requalification and functional requalification.

Intrinsic requalification checks the equipment that has undergone maintenance to ensure that it performs its function correctly. In general, intrinsic requalification is first carried out under ambient temperature and pressure conditions without any conditioning of the system that features the equipment in question; this check can only be fully completed by conducting final tests in the operational system configuration. Intrinsic requalification is intended to demonstrate that the equipment operates correctly prior to undertaking functional requalification.

Functional requalification must be carried out before the equipment is returned to operational service (more specifically, before it is required to meet reactor operating conditions). It consists in testing the overall performance of a functional system or subassembly made up of several components, including the equipment that has undergone maintenance work. System configuration is generally required to enable this test.

An item of equipment is returned to operational service once the required results of intrinsic and functional requalification have been obtained.

26.5.2. Main conditions for successful maintenance

Beyond obtaining the expected level of equipment reliability and performance, maintenance work must proceed under appropriate conditions of safety for the personnel involved. Moreover, maintenance work must not cause a reactor operating incident. This implies that maintenance personnel must proceed according to work procedures and comply with standard good practice for the discipline in question (which is not recalled in work procedures). Each of the steps (writing and adaptation of the maintenance baseline[702], preparation of maintenance operations, execution, requalification, experience feedback) must be carried out, as far as possible, according to the planned schedule in a calm, diligent and disciplined manner.

Faults of organizational or human origin (poor preparation of the maintenance file, poor preparation of the maintenance operation, non-compliance with conditions required to perform the work, poor handling or fitting error, etc.) or of material origin (inappropriate spare part, etc.) may result in non-quality maintenance (NQM). As mentioned at the beginning of this chapter, non-quality maintenance can cause not only immediate failures, but also failures that will only occur when the equipment is under load (latent failures).

Non-quality maintenance or failures may also result in deterioration or incidents such as the introduction of loose parts into the reactor coolant system, loss of a safety function under normal operating conditions or in an accident situation, to name a few.

The risks arising from non-quality maintenance depend on:

- the type of deviations, their latency time, kinetics and any harmful effects,
- the ability to detect deviations before they result in failure by means of monitoring and inspection programmes, periodic testing, etc.,
- the operating conditions under which the failures occur,
- the ability to mitigate failures by taking measures in the design phase (for example, loss of a system on one train compensated by performing the same function on the other train) or through operational measures.

It should be noted that non-quality maintenance (incorrect file, human error, inappropriate spare part, etc.) may be explained by more generic causes, thereby affecting several components. On discovering an instance of non-quality maintenance, the facility operator must analyse whether it is of an isolated or potentially generic nature.

Some of the necessary conditions for successful maintenance operations are described in detail in the illustrations below. Since, in terms of quality, results have not always been up to expectations, ongoing efforts are made to advance maintenance quality and detect room for improvement.

[702] The maintenance baseline includes the work procedures.

▶ An adequate and relevant maintenance baseline updated to take into account operating experience feedback

Maintenance strategies and the associated maintenance operations must be adapted to equipment deterioration modes while taking into account environmental conditions, which are a major influencing factor. The frequency of maintenance operations must be consistent with the predicted or observed deterioration kinetics.

For example, coastal facilities are particularly affected by corrosion, such as the major deterioration observed on the cooling water pipes of the emergency diesel generators at the Gravelines site. No maintenance work was planned for these pipes, but regular inspection and maintenance could have prevented this corrosion. Proper performance of these activities is all the more important given that this is equipment which must be capable of withstanding mechanical, and in particular seismic, loads. Following this incident, EDF updated the relevant maintenance baselines for this equipment in order to prevent such deterioration.

Like corrosion phenomena, other phenomena may also undermine equipment reliability under normal operating conditions or in an accident situation and should be reassessed according to the situations encountered in the facilities. Common phenomena include ageing due not only to natural causes, but also to excessive heating (ageing of polymers [such as those used in Silentbloc-type shock absorbers mounted on electrical cabinets or the anti-seismic pads for isolating reactors at the Cruas-Meysse nuclear power plant], capacitor ageing on printed circuit boards) as well as stress corrosion cracking in the reactor coolant system and vibration phenomena.

In general, the fact that no malfunctions have been observed on a component is not sufficient to justify that the equipment is not to be inspected. Furthermore, it is important that data collected from maintenance feedback be processed in a timely manner so that any shortcomings can be quickly addressed.

Examples of some specific items of reactor equipment for which the preventive maintenance policy did not initially have sufficient data include the rod cluster control assemblies (RCCAs) and the reactor vessel internals:

- wear on the RCCAs at Unit 4 of the Tricastin nuclear power plant was revealed in 1987 but did not result in a sufficiently rapid increase in preventive maintenance inspections; this led to control rod rupture in the assemblies at Dampierre-en-Burly and Gravelines (see Section 26.5.3);
- the discovery in 1987, during investigations carried out following damage to peripheral fuel assemblies caused by ‘baffle jetting’, resulting in deterioration of the baffle assembly screws at Unit 2 of the Bugey nuclear power plant brought to light shortcomings in the preventive maintenance carried out on reactor internal structures up until 1988. This precursor event was taken into account in the maintenance policy for these structures;

- damage to ball bearings on fuel loading machines that occurred while handling assemblies at the Tricastin facility in September 1987 and at the Saint-Laurent-des-eaux nuclear facility in November 1987 resulted in 3 mm diameter balls falling into the vessels. These events could have been avoided by better maintenance, and the lack of a maintenance programme for the fuel handling machine certainly played a major part in these events.

In conclusion, it is clear that maintenance policies must be adapted to take into consideration lessons learned from experience in reactor operation. It also appears necessary to anticipate in areas where experience is limited.

Therefore, in order to take into account developing knowledge on deterioration phenomena or the actual state of facilities, it is important for maintenance baselines to be periodically reassessed, in particular on the basis of operating experience feedback. Complementary Investigation Programmes can also be conducted to confirm assumptions regarding the absence of notable in-service deterioration in areas that are not covered by basic preventive maintenance programmes[703] or by specific maintenance programmes. They are implemented during periodic reviews (see Chapter 30).

A number of key points should be mentioned with regard to maintenance programmes, specifically:

- thoroughness of implementation,
- adequacy in light of operating experience feedback,
- the lack of basic programmes for certain items of equipment.

Most of the time incomplete application of a maintenance programme is due to the time delay between writing the programme and its actual implementation at the facility. In particular, the planned technical inspection resources are not always available at a site. For example, bench-testing of self-locking devices on piping has suffered due to delays in test bench development. The first acoustic inspection of bearing rollers on the low-pressure pumps of the safety injection system could only be carried out on site three years after distribution of the corresponding basic programme and revealed deterioration on the pump bearings that had not been detected by conventional vibration checks.

Furthermore, it is important for nuclear power plants to take into account any changes to baselines in a timely manner so that the work procedures used by personnel are up to date. For this purpose, in order to harmonize and control the 'incorporation' of local maintenance baselines, EDF launched two projects in the late 2000s, namely:

- collaborative preparation of practices and methods for each plant unit series,
- incorporation of baselines during reactor outage campaigns (instead of scheduling deadlines outside of these periods) in order to avoid disruption of reactor outage preparations.

[703] *Programmes de base de maintenance préventive*, PBMP.

▶ Adequate preparation and planning

The preparation and planning phases are key to ensuring that a maintenance operation takes place under appropriate conditions once all the necessary documents and resources have been defined and brought together.

A risk analysis must be carried out during the preparation phase in order to identify any risks associated with a maintenance operation, along with the associated countermeasures, so that any pitfalls that may arise can be avoided. Risks may be directly related to the maintenance operation or the environment in which the operation is to take place, or may involve coordinating the different specializations involved (mechanical technicians, electricians, chemists, valve and pump mechanics, operating crew, etc.). Hazard risks associated with the maintenance work must also be examined (introduction of foreign matter, hazards to adjacent equipment, flooding, etc.). The technical lead of the maintenance team uses this risk analysis as input to brief the team that will perform maintenance operations once the team has understood its mission. Likewise, depending on the potential impact of the maintenance work on safety or the 'process' itself, the risk analysis may also be shared between the maintenance team and the operating crew. The aim of sharing in this manner is to ensure that the maintenance team has understood the prerequisites of its mission, the compatibility between the relevant maintenance operations and the state of the facility, and the consequences of these operations on the equipment, systems and even any affected safety functions.

▶ Control of maintenance operations

Controlling maintenance operations requires compliance with procedures and best practice. It implies that the personnel involved has the required technical skills and the practical know-how that comes with experience. It assumes that the personnel correctly understands the role of the structures, systems and components, especially those that are important to safety, and the impact of their action on the 'process' or on the ability to maintain equipment qualification. Interface relations between specializations, mentioned above, must also be examined in depth in order to keep the work process under control.

Given the technological complexity of the specializations involved in automation systems, valves and rotating machines, it can take several months or even years for the personnel to obtain the required skills through training, tutoring and mentoring.

To avoid incidents during maintenance operations, EDF implemented 'human reliability improvement' practices starting at the turn of the millennium. These involve:

– before work begins, holding a 'pre-job briefing' between the personnel involved and the technical lead to anticipate potential problems and review their solutions,

– during work, pausing in the event of an unexpected situation, ensuring the use of 'structured communication' (see Section 25.3.5) between persons in the maintenance team, or between maintenance personnel and operators in the control room for tasks that may involve risk when maintenance work is resumed, and checking that all persons concerned understand how to proceed when performing any actions at risk before undertaking these tasks,

- after the work has been completed, debriefing of the maintenance team by the technical lead to identify any lessons learned, both positive and negative, in the course of the maintenance operations.

It is, however, important for everyone concerned, whether in preparing for or actually carrying out the maintenance, to maintain a critical and questioning frame of mind at all times in order to detect and remedy any unforeseen scenarios or incorrect baseline conditions (safety culture).

Deviations associated with maintenance activities include non-compliance with tightening torques, failure to replace seals or connectors after disassembly, connection problems and issues relating to maintaining component leaktightness.

There are also other families of errors (referred to as 'human maintenance errors'), most often caused by:

- confusion between plant units, systems, trains or equipment items (the consequences of these errors may be particularly serious, even going as far as complete unavailability of a safety function, in particular in the case of a train error): an available item of equipment can be made unavailable after performing an act that was initially intended for another item that is actually unavailable on another train;
- maintenance work conducted simultaneously on protection systems for two trains;
- routine operations carried out without taking precautions, such as setting up test conditions on the protection system of one train when there is a pre-existing fault on the protection system of another train;
- incomplete or poorly applied work sheets, leading to, for example, leaving a sensor or valve in a state that is not compliant with the operating configuration;
- inappropriate action taken on equipment items (sensors, valves, relays, electrical cabinets) during checks or corrective action;
- lockout measures applied to areas outside the work area;
- work conducted in rooms at risk – foreign matter introduced into system lines, etc.

Furthermore, using Temporary Measures and Devices[704] to carry out inspections or testing can lead to errors when returning equipment to a compliant state. Such measures and devices may include:

[704] See Section 22.2.2.

- mechanical devices (blind flanges, plugs or relief valve clamping devices),
- electrical measures and devices (disconnection of wires, modified sensor or threshold detector settings, jumpers, etc.).

The use of these Temporary Measures and Devices, which cannot be avoided due to the system design, is a possible source of failure for engineered safety systems and protection systems. Some of these devices may not be visible to the untrained eye and, if used on passive or standby systems, may go unnoticed by members of the operating crew. As mentioned in Chapter 22, EDF was prompted in the early 1990s to give careful thought to this matter in order to solve problems arising from the use of Temporary Measures and Devices.

▶ Prevention of common-cause risks on redundant equipment and avoiding generic faults

Common-cause failures may result in the complete loss of a facility protection function or an engineered safety feature. Over the period from January 1986 to December 1989, and more particularly in 1989, a number of events associated with non-quality maintenance that led to the complete loss of a protection function or engineered safety feature occurred in France and other countries. Some of these are mentioned in Chapter 22. They resulted in a campaign to reaffirm the importance of applying the measures recommended for avoiding these faults, for example, having different teams carry out work on redundant trains during a given shutdown and ensuring functional requalification after maintenance operations. Another way of limiting the occurrence of such faults is to organize maintenance operations on redundant equipment so that this activity does not involve the same components on different trains during a given shutdown.

The prevention of common-cause failures is part of risk analysis, which must define the associated countermeasures as necessary.

It is also mentioned in Chapter 22 that other common-cause failure risks may be caused by calibration or test devices. Correct calibration and availability of the appropriate equipment are necessary conditions. Events of this type have revealed the importance of taking special care of unique tools required to check the state of specific components on one or more plant units in a facility.

There are many kinds of measuring devices used for maintenance purposes: voltmeters, deadweight pressure testers, ramp generators (this type of generator was the cause of a significant event mentioned in Chapter 22 which occurred on 31 May 1990 at Unit 6 of the Gravelines nuclear power plant), boron meters, other devices used to check instrumentation and control channels. In particular, special attention must be given to standards used for any calibration operation that involves several sensors.

Furthermore, the high degree of standardization in the French nuclear power fleet makes it particularly sensitive. Consequently, any omissions in maintenance programmes or any error that may be repeated in the course of maintenance operations can have an impact on several reactors. The following examples illustrate this type of situation:

- the October 1990 event affecting Cruas-Meysse nuclear power plant Unit 4: deterioration of a small component (a damping washer) due to ageing led to the explosion of a 6.6 kV contactor cubicle, which in turn led to the loss of one of the two emergency-supplied switchboards (LHA) and to the loss of all engineered safety systems on this train while the reactor was at power;
- several events associated with lubrication anomalies (mixing incompatible ingredients, product ageing, product shortages, inappropriate products, etc.). To illustrate, in November 1991, a mixture of different types of grease led to the unavailability of both pumps on the residual heat removal system at Unit 1 of the Gravelines nuclear power plant. In March 1993, a mixture of different types of grease led to unavailability of the four pumps on the low-head safety injection system at the same site, together with three pumps on the containment spray system. Following these events, EDF took action to implement 'generic' measures. Safety organizations then emphasized the importance of considering greasing activities as high-risk operations that require adequate traceability from the moment these ingredients leave the store. Nevertheless, events of the same kind have occurred subsequently, as mentioned in Section 29.2.2.6.

Operating experience has furthermore revealed a number of cases, discovered by chance, of latent faults of a general nature associated with poor maintenance practices (in workmanship, requalification, etc.). The time elapsed between the moment a fault occurs (sometimes at several plant units) and the moment it is discovered is a major parameter in evaluating its severity in terms of safety and defining corrective action.

▶ Quality of subcontracted maintenance

EDF outsources a large portion of its maintenance activity (approximately two thirds), in particular for work performed during reactor outages. This was already apparent over the 2000-2014 period due to an increase in the volume of maintenance carried out to improve equipment reliability.

The Order of 10 August 1984 already required the facility operator to carry out supplier surveillance to ensure the quality of subcontracted maintenance activities involving systems important to safety. The INB Order of 2012 has tightened up these surveillance requirements. It specifies that surveillance must be carried out by the facility operator itself and that it must be proportionate to the importance to safety of the activities performed. The facility operator must submit the implementation procedures for this surveillance function (principles and organization, resources used) to the safety regulator.

Operating experience has revealed a number of factors that contribute to successful surveillance of subcontracted activities, namely:

- in the preparation phase: sufficient time must be allowed for the surveillance leads to prepare quantitative and qualitative surveillance programmes;
- in the implementation phase: the workload must be coherent with the hourly 'volume' of surveillance to be carried out and the relevant surveillance leads must be assigned only to these duties;
- in the operating experience feedback stage: sufficient time must be allocated to the surveillance leads to carry out debriefing of the activities under surveillance and to evaluate subcontractor performance.

It is clear from the above that, to be effective, surveillance must be carried out by professional staff with recognized expertise, who have received the resources required to perform their duties.

In light of the increasing volume of maintenance planned from 2015 onwards (due to extension of reactor operating lifetime, major refits, etc.) and given surveillance requirements (INB Order of 2012), the consolidation of subcontractor surveillance remains a key factor in limiting non-quality maintenance.

However, as emphasized in Chapter 25, while surveillance of subcontracted activities is important, proper joint preparation of these activities between EDF and its contractors remains essential.

▶ Relevance of requalification

On completion of maintenance operations, circumstantial action or engineering changes, equipment and system requalification is essential. This involves not only functional checks, but also verifying compliance with specific requirements that cannot be tested during normal operation: component leaktightness (electrical cabinets), adjustment of protection systems that remain on standby during normal operation (electrical protection devices, relief valves, blowout diaphragms, torque limiters, etc.).

Following maintenance operations, functional requalification must be carried out before the equipment is required to comply with operational limits and conditions, except when this is technically impossible. It is true that requalification is sometimes delayed when specific conditions are required to test certain equipment. This is the case, for example, when requalifying the steam generator auxiliary turbine-driven feedwater pumps, which must be supplied with steam. This implies that they can only be functionally requalified when the reactor has reached an operating domain in which steam pressure is sufficient in the steam generators. The operational limits and conditions stipulate, however, that the auxiliary turbine-driven feedwater pumps must be available in this operating domain.

The event that occurred in January 1997 at Unit 1 of the Tricastin nuclear power plant illustrates the need for and difficulty of defining a representative requalification test. Following the maintenance overhaul of a valve on the component cooling water system (CCWS), the valve was requalified, but only by testing actuation without any fluid flow. The test did not reveal that the valve gate had been inverted during installation. The anomaly subsequently became apparent when the valve was actuated and became jammed at full flow, even though, according to the facility operator, the orientation of the gate should not have interfered with the ability to actuate the valve. The intrinsic and functional requalification procedure defined by the facility operator was inappropriate for the maintenance operation performed.

Following a number of events that occurred in the 1990s and then 2000s, EDF changed its practices by establishing an initial requalification policy, followed by a methodology guide, so that each nuclear power plant could implement an approach that aims to improve adequacy between requalification tests and the maintenance operations performed.

Since the requalification tests to be carried out on completion of maintenance operations are defined on a case-by-case basis, attempting to ensure that they are exhaustive remains a constant concern for facility safety.

▶ Sufficient inventory of spare parts

The facility operator must be ready to take preventive action on reactor equipment before facility safety is affected or take curative action when an equipment item is defective. To carry out these operations within an appropriate turnaround time, spare parts in sufficient quantity and of a quality that is compliant with design requirements must be available. In this respect, the facility operator must organize spare parts storage to avoid damage, deterioration and ageing, in particular for those parts used in redundant or similar equipment items, so that they do not give rise to common-cause failures.

However, spare parts logistics and management (determining the necessary inventory levels, referencing, procurement, storage conditions, etc.) depend on the type of parts in question. For major passive components such as the reactor vessel heads or steam generators, the availability of spare parts or components is mainly determined by manufacturing lead times, which can be very long, as well as the manufacturer's skills and the necessary means required for manufacture.

For other active or passive components, replacing qualified equipment, which is frequently subject to technological or commercial obsolescence, requires foresighted procurement and demonstrating spare part qualification.

Undetected referencing errors (few in number in comparison with the considerable number of listed spare parts) have resulted in non-compliant spare parts being fitted, thereby resulting in reduced reliability of the relevant equipment.

One major factor to keep in mind regarding parts replacement during maintenance operations is maintaining their specifications and qualification. In the context of the inspection procedure for maintaining equipment qualification at Unit 1 of the Tricastin nuclear power plant, the first-off unit of the 900 MWe reactors, during the compliance review associated with its second ten-yearly outage, the facility operator discovered that polyamide cage bearings had been fitted on the pumps of the low-head safety injection system and containment spray system, whereas the maintenance manual specified the use of metal cage bearings. These bearings are sensitive components on the engineered safety pumps. One of the important functions of the pumps is to circulate water for an extended period following a loss-of-coolant accident and bearing non-compliance could jeopardize their operability. This deviation proved to be a general practice.

Furthermore, spare part shortages had led EDF to postpone maintenance activities, to install parts considered as equivalents but with a lower qualification level, or to refit a worn part and justify the acceptability of this temporary solution.

The aim of the investment made by EDF in the 2010s (creation of a national spare parts storage centre for efficient and responsive procurement, redefinition of safety stocks, etc.) was to establish robust spare part procurement for the various nuclear power plants, despite technological changes and changes in the structure of the industry. However, despite this investment, personnel working in nuclear power plants are still encountering problems with obtaining timely supplies of the spare parts they need. EDF is continuing its efforts in this area.

26.5.3. Examples of anomalies or deviations discovered during routine maintenance, explained by an inadequate maintenance baseline with regard to deterioration mechanisms

▶ Wear and swelling of control rods

Excessive wear together with swelling and cracking phenomena that could lead to jamming of rod cluster control assemblies in the fuel assembly guide tubes were observed on RCCAs as far back as the 1980s. These phenomena led EDF first, to change assembly design (by reducing the diameter at the bottom of the control rods, the area the most subject to swelling [see Figure 26.5], and applying a wear-resistant coating[705]) and second, to improve its maintenance programme and increase monitoring of these items. These actions have brought about a significant reduction in the risks of mechanical jamming of the rod cluster control assemblies and in reactor coolant system contamination from metastable silver-110 originating from control rod perforation.

The wear phenomenon affected shutdown RCCAs, which remain permanently in the raised position when the reactor is operational and are particularly exposed to vibrations brought about by hydraulic flows.

However, cases of incomplete RCCA insertion into the lower part of the fuel assembly guide tubes were observed at the 900 MWe (CPY) reactors starting in 2006. Analysis of these anomalies revealed that they were the result of faster than predicted irradiation-induced swelling which led EDF to modify maintenance strategy criteria in

[705] By ionic nitriding or electrolytic chromium plating.

2008 by limiting the service lifetime of rod assemblies and lowering the criteria for discarding materials. These new criteria have been applied to all the reactor series.

Since 2008, there have been no observed instances of RCCA jamming associated with swelling or wear.

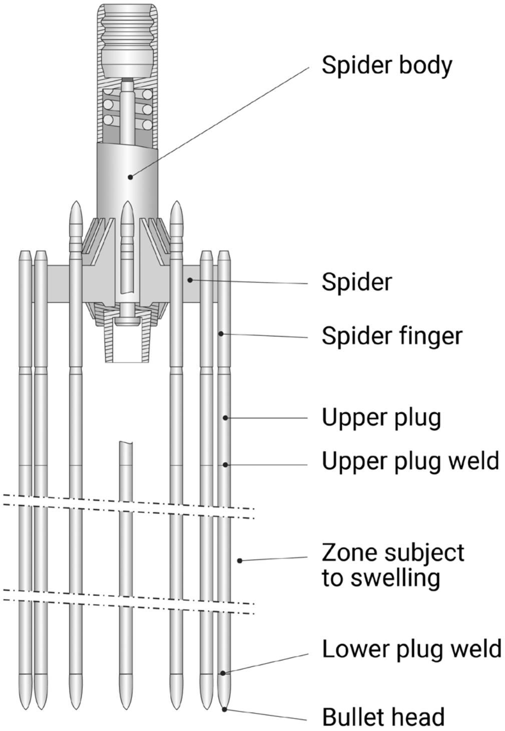


Figure 26.5. Diagram showing the zone subject to swelling in an RCCA. Georges Goué/IRSN.

▶ Equipment corrosion in coastal nuclear power plants: emergency diesel generators

In early 2008, inspections of the diesel-powered emergency generators at the Flamanville nuclear power plant revealed severe corrosion of the air coolers. These coolers, which are vital to proper operation of the diesel generators, are located outside the buildings accommodating the generators and are thus exposed to sea air. This phenomenon, already observed at a number of coastal power plants, shows that protecting metal surfaces with paint (see Figure 26.6) is only effective if accompanied by a specific inspection and maintenance programme.

An analysis performed by EDF revealed that traces of corrosion had been observed in 2006 but no corrective action had been taken. As a consequence, the Flamanville nuclear power plant reported a significant safety event on 18 April 2008.

Corrosion risks were taken into account in the design stage of the reactors, one of the solutions consisting of selecting materials which are not sensitive to corrosion, especially for equipment or pipes containing radioactive fluids. For other components, corrosion resistance is required not only due the nature of the fluid conveyed, but primarily because of environmental conditions. Protective measures using paint may be sufficient to protect metal surfaces. The effectiveness of these protective coatings must be checked periodically, however, because any deterioration in the paint may cause the equipment to be damaged through atmospheric corrosion, thereby jeopardizing reactor safety.

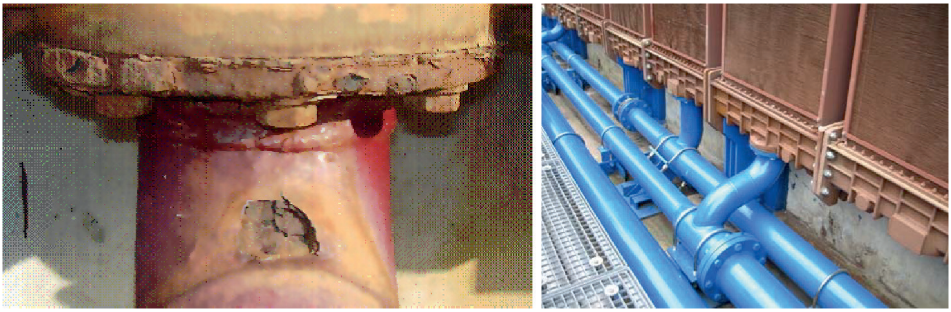


Figure 26.6. On the left, an example of external corrosion on a cooling pipe, a phenomenon that can ultimately lead to pipe perforation. On the right, an example of a corrosion-resistant coating applied on the outer surface of a cooling pipe.

Corrosion phenomena on diesel generators at coastal power plants was nothing new. As long ago as 1991, serious deterioration had been observed on generators at Unit 4 of the Paluel nuclear power plant in Normandy, i.e. just five years after it was commissioned. Due to poor design of the cooling system on the diesel generators for each 1300 MWe reactor, the presence of rainwater associated with maritime weather conditions caused patches of corrosion that were visible on the outer surface of the cooling pipes. EDF then quickly organized inspections on all 1300 MWe reactors. Deterioration of the same nature, but less advanced, had been noted at the Cattenom and Belleville-sur-Loire facilities despite the fact that environmental conditions at these sites were less aggressive than the saline coastal atmosphere. EDF then carried out the necessary repairs and remedied the generic design fault.

In April 2003, during an inspection at the Gravelines site, ASN also noted signs of corrosion on the cooling system piping of the diesel generators, leading to the inspection and repair work carried out in late 2003. In September 2003, EDF made similar findings at Unit 4 of the Paluel nuclear power plant. This corrosion, associated with the maritime environment, was treated in the course of normal equipment inspections.

All these observations revealed a maintenance programme in need of improvement and upgrade action taken with significant delays.

Despite measures taken to improve the situation, corrosion is repeatedly observed in coastal environments.

26.5.4. Examples of events associated with non-quality maintenance

The examples presented above and in the chapters devoted to operating experience feedback show that managing maintenance operations can be complex. Some additional examples are presented below; they illustrate the variety of non-quality maintenance situations and the need for the facility operator to make continuous efforts to ensure that maintenance operations do not introduce new anomalies in real-life maintenance situations where operations cannot always be conducted according to procedure due to organizational or material circumstances.

26.5.4.1. Example of an event explained by an incorrect setting on redundant equipment

▶ Valve calibration errors

(Golfech Unit 1 – 15 September 1999)

During an outage at Unit 1 of the Golfech nuclear power plant, when the safety injection system accumulator RIS 303 BA was placed under nitrogen pressure, valve RIS 273 VZ opened at a nitrogen pressure several bars lower than the rated operating pressure of the accumulator. An inspection of the other pressure relief valves that had been calibrated by the same contractor during the outage revealed that 22 pressure relief valves belonging to different systems showed calibration deviations of up to 6 bars.

The same individual had calibrated 18 of the 22 pressure relief valves because the contractor was understaffed at the time. The pressure relief valves were calibrated using a misadjusted measurement scale on the calibration bench because the technician was unfamiliar with the procedures for using the bench and did not have access to instructions on how to use it. Furthermore, the inspection procedure had not uncovered these deviations.

26.5.4.2. Example of an event explained by an incorrect setting of electrical protection thresholds

▶ Loss of heat sink and charging pump on train A

(Nogent Unit 1 – January 1999)

A significant safety event was caused by overload tripping on both pumps of the essential service water system and on the charging pump of the chemical and volume control system (CVCS) on train A during islanding tests at Unit 1 of the Nogent-sur-Seine nuclear power plant on 24 January 1999. Investigations conducted by the facility operator after the event revealed that the intensity thresholds had been set to a value lower than that specified, in particular on all the equipment supplied by the 6.6 kV switchboard of train A (11 actuators, including those of the engineered safety pumps).

This event is described in Section 23.1.1.1.

26.5.4.3. Examples of events explained by a failure to return equipment to a compliant state after maintenance or an error in performing a work procedure

▶ Unavailability of the CVCS letdown line due to the presence of water-soluble paper clogging the letdown orifices

(Flamanville Unit 1 – June 2008)

On 19 June 2008, when Unit 1 of the Flamanville nuclear power plant was restarting after a core refuelling shutdown, with the reactor coolant system in single-phase state and cooled by the safety injection system in residual heat removal mode, the operating crew noted an insufficient flow rate in the letdown line from the reactor coolant system to the CVCS. Assessments revealed the presence of clumps of paper (see Figure 26.7) that were clogging a large portion of the letdown orifices in the letdown line (multi-stage diaphragms). This paper had been used during welding of heat exchanger pipe connections upstream of the diaphragms.

The procedure calling for the use of water-soluble paper that had been applied by the contracted teams responsible for the heat-exchanger connection welds was incriminated in this event. Inappropriate positioning of the water-soluble paper (plugging the pipe at a distance that was too close to the weld) had caused the paper to lose its water-soluble properties.

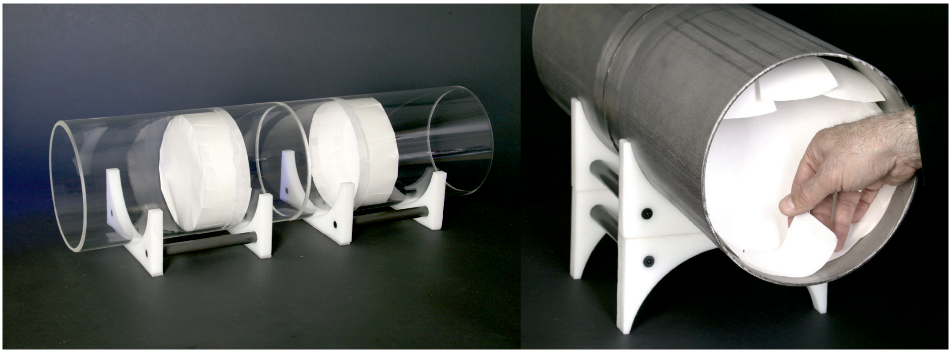


Figure 26.7. Two views showing water-soluble paper dams. Courtesy of Aquasol Corporation.

The actual impact on safety (letdown line unavailability) was immediately addressed by the operating crew. In the event of an accident situation resulting in isolation of the residual heat removal system, unavailability of the letdown line would have prevented the reactor coolant system in the single-phase state from being protected from cold overpressure.

This event highlighted the need to take appropriate measures to prepare for welding operations on piping important to safety, particularly when using water-soluble paper.

▶ Presence of alumina in compressed air systems

(Cruas Unit 2 – January 2013)

In January 2013, due to the presence of alumina powder, malfunctions affected two pneumatic (gate) valves (see Figure 26.8) on the moisture separator-reheater system on the Unit 2 turbine generator of the Cruas-Meysse nuclear power plant, as well as a compressor and its solenoid valve on the supply line of the compressed air production system.

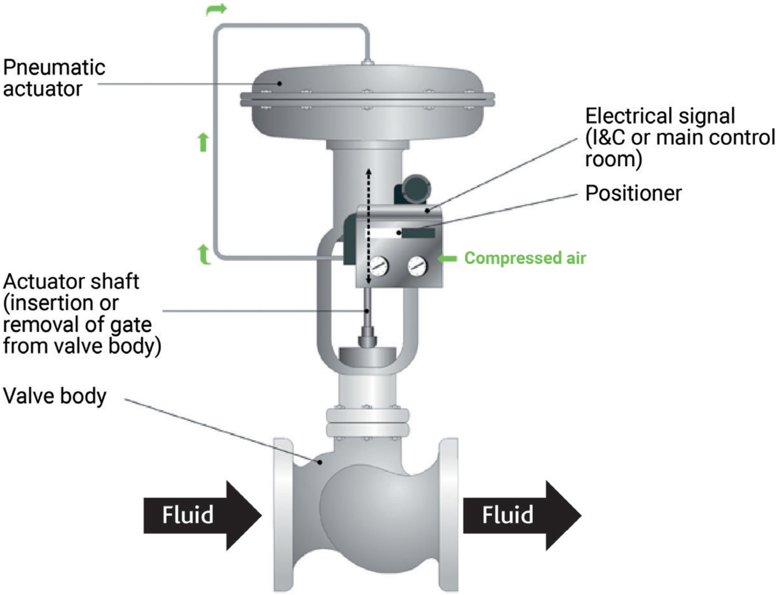

Pneumatic actuator
Electrical signal (I&C or main control room)
Positioner
Compressed air
Actuator shaft (insertion or removal of gate from valve body)
Valve body
Fluid
Fluid

Figure 26.8. View of the control mechanism on a pneumatic valve. Georges Goué/IRSN.

The most recent maintenance operations conducted on a dryer of the compressed air production system and on the two filters located upstream and downstream caused contamination of the compressed air production and control systems. This is because, in the course of these ordinary preventive maintenance operations, the procedure for replacing the alumina in the dryer was not observed, causing the alumina beads to break down into powder. Since the two filters were not leaktight due to insufficient tightening and a screen size that was smaller than the specified size on the upstream filter, the alumina powder was dispersed in the supply pipes to pneumatic valves along pathways where compressed air consumption is the highest. This was the case for the continuous-operation control valves in the main feedwater system, the turbine generator steam supply control system and the condensate extraction system, in particular.

The alumina powder had reached a large number of valves that were not protected by filters fine enough to capture the alumina particles. These particles then accumulated in the positioners that control the supply of compressed air to the pneumatic actuators according to the configured set point, leading to impaired operation of the valves.

The facility operator has implemented an in-service monitoring programme for the relevant valves. A major programme of inspection and cleaning of most of the pneumatic piping and valves on systems important to safety was carried out during the following scheduled refuelling shutdown.

Chapter 27
In-service Monitoring and Inspection of Equipment

As explained in Chapter 6, in-service monitoring and inspection of equipment important to safety (metal structures, civil works, etc.) constitute one of the components of defence in depth. There are two types of provisions:

- equipment and procedures for in-service monitoring of a number of reactor operating parameters, which can be used to assess the state of equipment, either directly or indirectly,
- periodic tests (for 'active' equipment) and direct equipment inspections (see the Focus feature further on), generally carried out during unit outages (sometimes during the ten-yearly inspections), under various programmes such as the basic preventive maintenance programmes[706].

These measures generally aim to manage equipment ageing in a broad sense, i.e. the effects of different damage mechanisms – or pathologies in the case of concrete structures – that are likely to affect the equipment over time or as a result of its use (in normal operation). Gradual damage to equipment is caused by operating stresses and the equipment environment (pressure, temperature, thermal transients, vibrations, irradiation, chemical interaction with the surrounding environment, etc.). Operating experience, particularly the results of in-service inspections, shows that unacceptable damage can occur even if damage mechanisms (those that are known) are taken into

[706] *Programmes de base de maintenance préventive*, PBMP.

account in the design, manufacture, and operation of equipment. Some examples are cracking on vessel head adaptors and steam generator tube bundles, topics that will be discussed further in later sections.

Ageing management relies not only on in-service monitoring and inspection but also on prediction. Several areas of research and development on the subject, which were expanded when Électricité de France (EDF) stated its intention of continuing to operate reactors beyond 40 years (the Operating Lifetime project), are discussed in Chapter 39.

This chapter[707] uses several of the most notable examples to illustrate how in-service monitoring and inspection of certain equipment in French nuclear power reactors have contributed to reactor safety. The anomalies found and the way they were dealt with are explained in detail. Anomalies discovered on pressurized water reactors in other countries (USA, Belgium) are also discussed. The measures taken to guarantee a sufficiently high quality of equipment manufacture[708], which are obviously extremely important (particularly for the first level of defence in depth), and also anomalies that can be found at this industrial stage and the way they are managed are not discussed in detail in this document; however, aspects of the manufacture of certain components (such as the reactor vessel) are explained in order to clarify certain anomalies encountered in service later on.

Fuel is a ‘consumable’ in pressurized water reactor operation; monitoring of its condition by checking the radioactive content of the reactor coolant system water, the anomalies observed and the changes made to its design are discussed in the next chapter.

It is important to note that the failure (or more specifically, the fast fracture) of certain large-scale equipment items at nuclear power plants is ‘excluded’[709]; the equipment items concerned are:

- the reactor vessel[710],
- the volutes on the reactor coolant pumps,
- the steam generator shells.

The rupture of steam pipe sections between the containment and the main isolation valves (also known as ‘protected sections’) is also excluded.

[707] Various sources were used for this chapter, particularly the very exhaustive publication entitled *La maintenance des centrales nucléaires* (Maintenance at Nuclear Power Plants) by Jean-Pierre Hutin – EDF/Lavoisier Tec&Doc, 2016, which is quoted several times in this book. The article *Confinement. Enceintes* (Confinement and Containment) by Jean-Louis Costaz, in *Techniques de l’ingénieur*, ref. B3290 V2 from 1997 was also used.

[708] Whether by the designer, manufacturers or inspection bodies (particularly the Nuclear Pressure Equipment Division in the case of the main primary system and main secondary system in nuclear steam supply systems).

[709] See Section 8.2.2.

[710] Including the nozzles and the closure head.

This means that the design, manufacture and operation of this equipment must meet high quality standards so that it remains compliant with the specifications defined when it was designed. During the operating period, this means looking carefully, using available effective inspection techniques, for the initiation of any degradation and, where appropriate, carrying out repairs as early as possible.

The aim of in-service monitoring and non-destructive testing is to check that these standards are met – in addition to the regulatory hydrotests, which are carried out to confirm the overall 'state of health' of the equipment, but which can also reveal defects in areas that are not tested or are difficult to test.

Steam generator tubes deserve particular attention. Their rupture is not excluded in the deterministic safety analysis, but it could lead to releases to the atmosphere that, though small, are clearly undesirable[711]. For this reason, safety organizations have reminded EDF several times of the importance of fuel rod integrity and therefore of sufficiently tight operating limits being set for radioactivity in the reactor coolant system water.

Some of the equipment discussed in the rest of this chapter is nuclear pressure equipment[712]. Inspection programmes for this equipment have been defined as part of the application of the pressure equipment regulations for nuclear power plants; examples are the Facility Operation Order of 10 November 1999 mentioned in Chapter 2, which is still applicable, and the Pressure Equipment Order of 2015, amended in 2018.

To justify leaving untreated any defects discovered during the operation of equipment in the main primary system and the main secondary system of a pressurized water reactor, the risk analysis for fast fracture of the equipment requires safety factors to be taken into account for category 2, 3 and 4 situations (as defined in pressure equipment regulations)[713], in accordance with Article 11 of the Facility Operation Order; these factors are given in the table below.

Risk analysis for fast fracture of the equipment	Situation categories according to pressure equipment regulations[714]		
	Second category	Third category	Fourth category
Risk of onset of tearing	1.3	1.1	No specified factor
Instability risk	2.0	1.6	1.2

[711] This type of accident, originally classed as a Category 4 operating condition, was then reclassified as Category 3 for design studies, which was applied starting with design studies for the N4 series.

[712] Information gathered in collaboration with Simon Liu at ASN/DEP and Remy Catteau at ASN/DCN.

[713] The propagation of defects during the period in question must also be considered.

[714] Factors are not specified for second category situations, but the 1974 order nevertheless stipulates that the "manufacturer will show that […] the equipment does not present any risk of gradual deformation or gradual cracking during the expected period of use" of the equipment.

The Facility Operation Order specifies that "cracks detected must be eliminated unless specific appropriate justification is provided"; as a matter of principle, planar defects must be repaired.

Since 26 February 1974, the date of the order enacting pressure equipment regulations applicable to nuclear steam supply systems, feedback from in-service inspections and the improvement of detection instrumentation has led to unexpected findings, starting from the late 1970s. These involved both the reactor vessel ('underclad defects', cracking of vessel head adaptors linking the rod cluster control assembly drive mechanisms to the vessel) and the 'protected sections' (defects affecting the welds of valve takeoffs from the main pipes), as well as the steam generator tubes. Safety organizations therefore decided that it was necessary to conduct inspections that were as regular and exhaustive as possible.

The operator obviously aims to limit the duration of inspections performed during unit outages and to keep radiological exposure of inspection personnel to a minimum. It therefore seeks to optimize in-service inspection by determining the best way to adapt inspections to the risks of equipment alteration, taking into account what is known about the damage potential in each area and what has been observed up to now. This could mean, for example, applying sampling inspections across the entire fleet of reactor vessels or pressure equipment on reactor coolant pumps. It was considered, however, that this approach would not be compliant with the 1974 order because it was based on the assumption that exhaustive knowledge of equipment degradation possibilities was available and that the characteristics of the materials or manufacture of all equipment of a particular type were fully known, which experience had shown was not the case.

Moreover, defence in depth means considering not just defects in places where they are most likely to occur based on mechanical criteria or current knowledge of a damage mechanism, but also in places where the consequences would be particularly harmful from a safety point of view. The example of vessel head adaptors provided particularly valuable lessons in this respect.

The importance to safety of the cracks discovered in a vessel head adaptor at Unit 3 of the Bugey nuclear power plant, presented in this chapter, confirms the benefits to be gained from conducting an overall test programme on the main primary system. These tests can reveal defects in areas considered not to be loaded to the point of fatigue and that are therefore not specifically monitored (if there is nothing that indicates a risk of early corrosion).

The above considerations also prompted EDF to set up 'complementary investigation programmes'[715], which consist of conducting sampling inspections on equipment items (pipes, tanks, etc.) that are not inspected as part of maintenance programmes, regulatory inspections (pressure equipment) or special inspections carried out when

[715] These programmes are discussed in Chapter 30 on periodic reviews.

generic or specific deviations or problems are found, because they were not considered to be sensitive at the time of the design studies.

It should be noted that the main primary system and main secondary system of French nuclear power reactors are monitored by means of 'situation logging'. This consists of recording the values reached by certain reactor operating parameters, thereby tracing the loads applied to the various components in these systems over time (in terms of temperature, pressure, duration, etc.) in order to ensure that these loads remain within the bounding case defined by the situations and possible damage modes (excessive deformation, fatigue, etc.) included in the design basis. The contribution made by fatigue testing of these systems is small and is taken into account during component design. At the end of the originally planned 40-year operating lifetime, past 'situation logging' results will be used, along with many other data, to demonstrate that the equipment is fit for continued reactor operation.

Finally, in the case of mechanical or electrical equipment that can be repaired or replaced, preventive maintenance can keep defects from occurring.

#FOCUS

Overview of different techniques for direct inspection of equipment

Direct inspection of equipment can be carried out in various ways; a brief explanation of some of them is given below.

Non-destructive testing (NDT)

Several non-destructive testing techniques are used:

- Visual inspections. Their effectiveness varies and depends on many factors. In some cases, visual inspection has been slow to detect defects, for example, in March 2002, when boron crystals were observed on the outside of the reactor vessel at the Davis-Besse nuclear power plant in the USA, cracking on the vessel head penetration was already quite extensive (with thinning in an area on the carbon steel vessel head). Performance can be enhanced by using endoscopes, or remote observation; advances in the miniaturization of imaging devices, like those in smartphones, means that very good images can be obtained with very small devices.
- Liquid penetrant testing is a specific non-destructive testing method. In the first phase, the surface of a metal part is impregnated with a coloured or fluorescent fluid, then in the second phase the part is wiped and a developer is applied. It can be used to detect the presence of defects on the surface examined but it cannot determine their depth.

- Magnetic particle testing. This process consists of depositing fine, coloured or fluorescent ferromagnetic particles on the surface of a part and applying a magnetic field. Any surface discontinuities deflect the magnetic flux and cause magnetic flux leakage which attracts the particles and thus indicates the presence of any surface or near-surface defects in the part. Magnetic particle testing has the same limitations as liquid penetrant testing in terms of characterizing defects.

- Radiographic testing. Radiography consists of obtaining an image (on silver film or as a digital image, depending on the technique used) of the material density of a part through which X-rays or gamma rays pass. It can detect all types of cavities or foreign matter included in the part (inclusions) and any planar discontinuities that lie parallel to the emitted rays. The limitation of this process is that it cannot determine the depth of planar defects perpendicular to the surface, which are often the cause of most concern. It is not really affected by the surface condition of the part.

- Ultrasonic examination. This process is based on the propagation and reflection of an ultrasonic wave within a part. The waves are emitted by one or more sensors, known as transducers, deployed by an operator or an automated system (as in the case of the reactor vessel inspection machine used at French nuclear power plants). By processing the signals received, it is possible to determine the position of defects and to characterize them (dimensions and type). This process can find defects both on the surface of a part and inside it: planar defects are particularly easy to detect when the ultrasonic wave is orthogonal to them. The performance of this technique depends to a great extent on the metallurgical structure of the material (a material with an anisotropic or heterogeneous metallurgical structure can deflect or disperse the ultrasonic beam). This process is generally suitable depending on the type of defect expected, as well as the geometry and accessibility of the part in question; development work is being carried out in this area (see Figure 27.1).

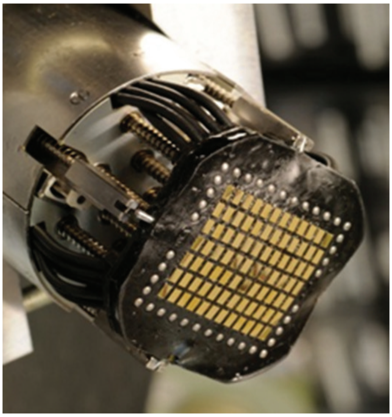


Figure 27.1. Prototype of a ‘conformable’ multi-element ultrasonic probe – IRSN/CEA patent. IRSN/CEA.

– Eddy current examination. This process consists in creating currents induced by a variable magnetic field in an electrically conductive material, using a probe containing an exciter coil. When there is an anomaly in a part being inspected using this process, circulation of the induced currents is disrupted, leading to variation of the apparent impedance in the probe, depending on the type and size of the anomaly. Analysis of this variation provides information that can be used to characterize the defects. This process, which is very sensitive, is ideally suited to the detection of defects (cracks, wear, etc.) on the surface of parts (or inside them if they are not very thick, as is the case for steam generator tubes).

The above processes obviously need to be qualified by means of preliminary tests on test specimens representative of the parts to be inspected (type of material, geometric shape, etc.); the qualification process can be long and complex. The development of numerical simulation[716] can provide valuable support in this area.

Inspections requiring equipment dismantling

Equipment may require partial or complete dismantling for a detailed assessment (or inspection), particularly in areas that might not have been inspected using one of the above techniques prior to dismantling.

Destructive testing (or examinations)

In some cases, destructive testing may be carried out: taking cores from civil works, cut-outs from (replaceable) dismantled components, etc.

27.1. Main internal equipment items on a pressurized water reactor vessel

Figure 27.2 below shows a diagram of a pressurized water reactor vessel, except for EPR, and some of its equipment.

[716] For more information, see Section 10.1.2 of Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

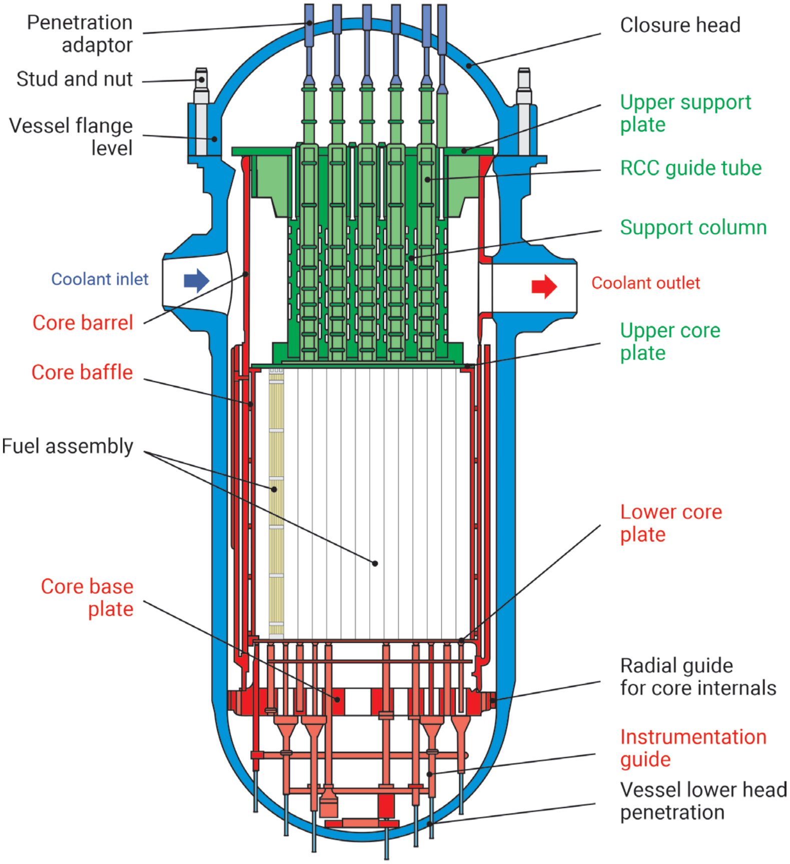


Figure 27.2. Cross-sectional diagram of the vessel (blue) and its lower internals (red) and upper internals (green) in a pressurized water reactor. Diagram taken from *La maintenance des centrales nucléaires* (Maintenance at Nuclear Power Plants) by Jean-Pierre Hutin – EDF/Lavoisier Tec&Doc, 2016.

27.1.1. 'Core baffle' around the core

The equipment or structures inside the vessel of a pressurized water reactor (the 'internals') are formed by a bolted and welded assembly that performs various functions:

- it supports the fuel assemblies (lower internals),
- it holds the top of the fuel assemblies in place and guides the rod cluster control assemblies (upper internals),
- it directs the coolant flow used to cool the core.

A hold-down spring is placed between the two sets of internals. The complete assembly is secured by the vessel closure head, once it has been tightened.

In terms of safety, the internals carry out several functions:

– they support the fuel assemblies and secure them in place,

– they distribute coolant throughout the vessel and core,

– they ensure the insertion of the rod cluster control assemblies and the core instrumentation by maintaining their alignment with the fuel assemblies,

– they protect the vessel from the gamma and neutron radiation emitted by the core,

– they support the thermal instrumentation and the irradiation specimen capsules (the role of these specimens is explained further on).

Among the lower internals, the core baffle consists of a set of long, narrow plates (baffle plates) installed vertically inside the core barrel and assembled so as to form a polygonal boundary that fits around the square shape of the fuel assemblies. The baffle plates are secured to the core barrel by means of horizontal spacers (former plates), featuring holes for the water to pass through. The arrangement is assembled and secured using bolts.

In the first French reactors, it was originally 'cold' water that passed between the core barrel and the baffle, in a downward flow. This created a difference in pressure and temperature on either side of the baffle, inducing stress on the bolts, creating gaps where the baffles meet with crossflows through these gaps, and inducing vibrations in the fuel assemblies (referred to as 'baffle jet'). As of 1981, degradation of fuel rods[717] around the edge of the core was observed in the first units (Fessenheim and Bugey nuclear power plants [CP0 group]). EDF dealt with the problem by modifying the design to reverse the flow of water between the baffle and the core barrel (from a downward flow to an upward flow, referred to as the 'up-flow conversion'), thus eliminating the difference in pressure and temperature on either side of the baffle.

However, damage to the bolts, made from type 316 austenitic steel, was still an issue. Ultrasonic tests were carried out from 1988 onwards at the Fessenheim and Bugey reactors; slightly more than 150 bolts (out of thousands) were found to be damaged and were replaced. The cause of the problem was irradiation-assisted stress-corrosion. For the next 900 MWe reactors (programme contracts CP1 and CP2), and the 1300 MWe and N4 reactor series, further design improvements were adopted to improve bolt cooling and reduce the thermal-mechanical stresses to which they were subjected (by adapting the bolt design and grade of steel and reducing the tightening torque).

Periodic inspection of the baffle-plate bolts has nonetheless been maintained.

[717] This degradation caused fuel to leak into the reactor coolant system.

27.1.2. RCCA guide tubes

The RCCA guide tubes guide the RCCAs during their upward and downward movements. Each guide tube consists of a housing with openings in the lower part to enable the water from the reactor coolant system to flow to the vessel outlet nozzles. Inside there are devices that guide the assembly control rods. The lower end has a base plate to which are bolted two split pins, which are inserted into holes in the upper core plate to keep the RCCAs aligned with the fuel assemblies, while leaving the guide tubes free to expand.

Cracks and ruptures of guide tube pins were observed from 1982, particularly at the Gravelines nuclear power plant where a check valve was found to be blocked by foreign matter, which turned out to be a piece of a pin. Checks on all units showed that this was a generic problem. Cracking on pins, which were made from a nickel-based alloy (X750), was attributed to a stress-corrosion mechanism. From 1982 to 1985, a new generation of pins was installed in the reactors. But another event in 1987 at the Tricastin nuclear power plant (a piece of pin found in a steam generator channel head) cast doubt on the suitability of these new pins. Subsequently, various new generations of improved pins were gradually installed, up to the fifth generation which had a suitable grade of steel, fewer fabrication and tightening constraints, an improved design and better sequencing of the fabrication operations. EDF nevertheless maintained in-service monitoring measures and inspection programmes at all its reactors to detect any failures on the new guide tube pins.

27.2. Reactor vessel, nozzles and head

All the reactor vessels at French nuclear power plants were manufactured by Framatome from forged parts supplied mainly by Creusot-Loire, including the vessel shells. The vessel shells are made from ingots cast at a steel plant, and their manufacture is a complex process (see Figure 27.3) involving various different forging operations:

- cropping the ends of the ingot to remove the zones containing impurities,
- drilling the ingot (in the case of a solid ingot),
- drawing the blank on a mandrel,
- shaping[718].

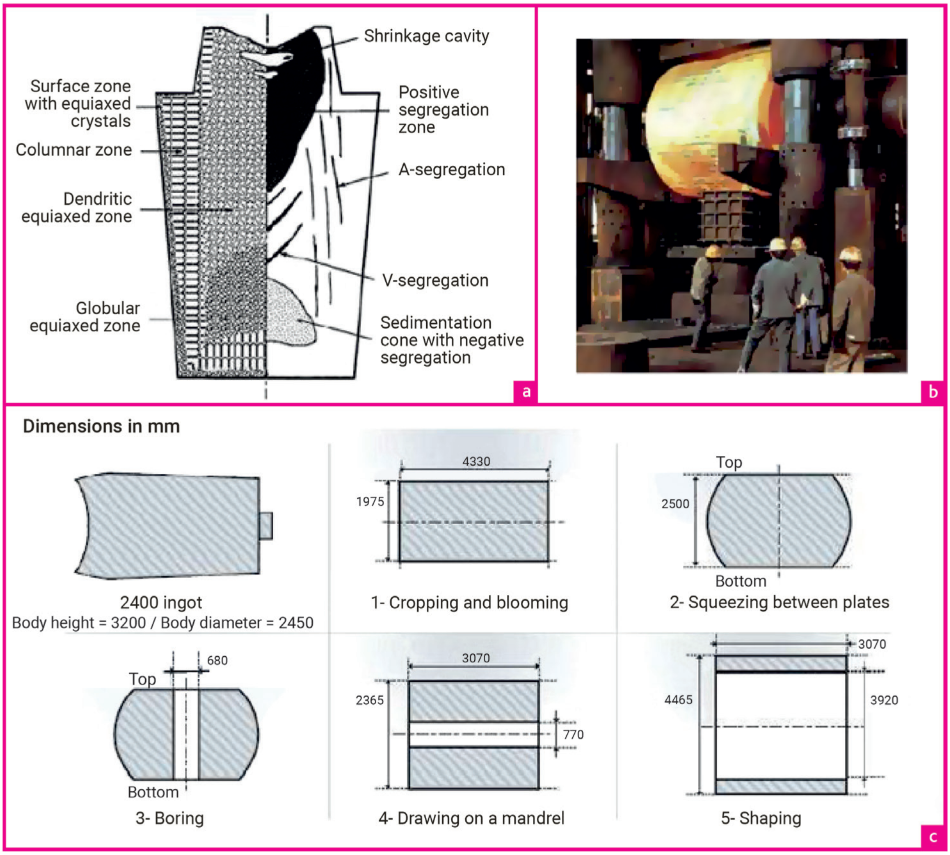
During these operations, most of the impurities and the macrosegregation[719] are eliminated. After these hot working operations, the forged parts are fully tested using

[718] Increasing the diameter.

[719] Heterogeneities in local concentrations of chemical species. For example, a higher than expected carbon concentration in some parts of the vessel (head and lower head) of the Flamanville 3 EPR was reported to safety organizations in 2014. EDF and Areva carried out analyses to find out whether forged parts installed in any nuclear power plants in operation might be affected by these heterogeneities. These analyses showed that an anomaly of this kind could affect 46 steam generators with lower heads manufactured by Creusot Forge and Japan Casting & Forging Corporation.

an ultrasonic testing process to find any defects (flaws, cavities, inclusions[720], cracks, etc.). This can lead to the part being scrapped if the criteria are not met. The different parts are then assembled by welding. The welds are also fully tested using two different testing processes (radiographic and ultrasonic testing). The stainless steel cladding is welded to the internal wall of the vessel in two stages.

Once the vessel has been assembled, the main operations to be carried out are factory hydrotesting, required by French regulations, and shipping to the site. From a regulatory viewpoint, fabrication is monitored from the start by the French Ministry of Industry's Inspectorate of Nuclear Steam Supply Systems[721], which became the Nuclear Inspection Agency and then the Nuclear Pressure Equipment Department[722] within the French Nuclear Safety Authority (ASN).



a : Segregations in an ingot; b : Shaping a 900 MWe vessel shell; c : Forge procedure for shell on 900 MWe reactor

Figure 27.3. Standard procedure to forge a shell for a 900 MWe reactor from a solid ingot. IRSN.

[720] Undesirable metallic or non-metallic materials in a metal or alloy.

[721] *Bureau de contrôle des chaudières nucléaires*, BCCN.

[722] *Direction des équipements sous pression nucléaires*, DEP.

27.2.1. Vessel underclad defects

Small planar defects can be created in the ferritic steel when the vessel cladding and nozzles are installed, under the layers of austenitic steel. They can be caused by two mechanisms, cold cracking and intergranular reheat cracking. The defects are a few millimetres in size.

Cold cracking[723] occurs in the 'heat-affected zone' of a weld, as the result of a combination of hydrogen embrittlement and major stresses caused by cooling after welding. The defects are transgranular[724]. Defects of this kind were detected in 1978 in steam generator tubesheets (also lined with austenitic steel), then in some vessels during fabrication, around their nozzles; they were planar defects perpendicular to the vessel's internal wall. These were the first 'underclad defects' discovered in vessels. The components being fabricated at the time were repaired and the fabrication procedures were modified to prevent these defects, but some vessels were already installed on sites.

EDF mapped all vessel underclad defects, particularly those in the beltline region[725], on all the vessels in question. Studies have shown that, in view of the dimensions of the defects detected, the fabricated parts complied with regulatory safety coefficients. The decision was made to leave them as they were, since repair would be very difficult. These defects are protected from corrosion by the cladding and any fatigue stresses in the zones concerned are very small.

In-service inspection programmes include ultrasonic examinations focusing on welds and adjacent areas to find any defects resulting from the fabrication process anywhere in the vessel's thickness. EDF has developed ultrasonic probes capable of detecting and characterizing very small defects (typically 5 mm) in the ferritic steel just under the cladding. From 1989 onwards, this technique was used during complete examinations to inspect a section, then very quickly the entire beltline region (the only area where irradiation-induced embrittlement could make underclad defects a real cause for concern). Several generations of ultrasonic processes have been used in turn for signal acquisition and processing, and performance has continually improved: the First Thirty Millimetres process, First Twenty Millimetres process, then the beltline

[723] Much of what follows is taken from the book by Jean-Pierre Hutin cited at the beginning of this chapter (Chapter 10, Sections 1.3 and 4.1 of the book). Other anomalies are mentioned in this book, concerning the bimetallic bonds (welds) used to join large, lined ferritic steel components to the austenitic stainless steel pipes of the main primary system. These bonds are inspected with particular care at the fabrication stage because they must be demonstrated to be unbreakable throughout the reactor's life. Fabricating these bonds involves a sequence of operations to ensure the materials are weldable, starting with buttering of the lined ferritic steel part then filling of the bevel between the buttering and an austenitic steel weld edge. A last post-weld heat treatment is carried out at the final stage of fabrication to improve the ductility of the heat affected zones. This also plays a part in redistributing residual stresses.

[724] Crossing the grains of the material. Defects are described as intergranular when they are between the grains.

[725] See Section 27.2.4. Monitoring of the 'beltline' region of the vessel.

process. They are all carried out by the in-service inspection machine (see Figure 27.6 for an image of one of these machines).

About 20 signs classified as underclad defects were detected and characterized across all French reactor vessels, with Tricastin Unit 1 appearing to be the most affected. Successive inspections confirmed that there have been no changes.

Intergranular cracking occurs in the heat-affected zone and is associated with forging, successive welding layers or later stress-relieving treatments. The size of the resulting defects is limited to the size of the heat-affected zone (which has a coarse-grained structure). This type of defect is parallel to the surface of the part and is known as 'intergranular reheat cracking' (caused by decohesion). Intergranular reheat cracking was discovered in vessel shells when checking the effectiveness of measures taken to remedy underclad defects. As soon as the conditions leading to these anomalies were identified, preventive measures were taken during fabrication. But many vessels already in service did not benefit from these measures.

It was first thought that only intergranular reheat cracking could form in the vessel shells, but some of the defects detected (those found in vessels at the Saint-Laurent-des-Eaux and Tricastin nuclear power plants) suggest that the vessel shells can also be affected by cold cracking. Conversely, the geometry of the vessel nozzles makes them more vulnerable to cold cracking, but intergranular reheat cracking has also been found in them.

In-service monitoring of these defects has benefited from the developments mentioned earlier for underclad defects.

27.2.2. Cracking on vessel head adaptors

In September 1991, a small leak was detected in one of the vessel closure head penetrations at Unit 3 of the Bugey nuclear power plant, during hydrotesting of the reactor coolant system of this unit as part of the regulatory ten-yearly outage. This 900 MWe reactor, commissioned in 1979[726], had totalled about 80,000 h of operation.

Once the fuel assemblies had been unloaded, the hydrotest was carried out at a pressure of 207 bars and a temperature approaching 80°C (the normal operating pressure of the reactor coolant system is 155 bars). The detected leak, of about one 1 L/h, affected one of the 65 leaktight adaptors (see Figure 27.4) that accommodate the rod cluster control assembly shafts and the instrumentation for core temperature measurement, which pass through the reactor vessel closure head. The affected adaptor was at the edge of the vessel closure head; like the others, it was made of a nickel-based alloy from the alloy 600 family[727].

[726] It was connected to the electricity grid in 1978.

[727] This material contains nickel, 15% chrome and 10% iron. The term 'alloy 600' will be used by preference in the rest of the text in reference to different metals belonging to the alloy 600 family, instead of 'Inconel 600', since Inconel is a registered trademark of the Special Metals Corporation used to refer to various metal alloys; the same will apply to other grades (such as alloy 690).

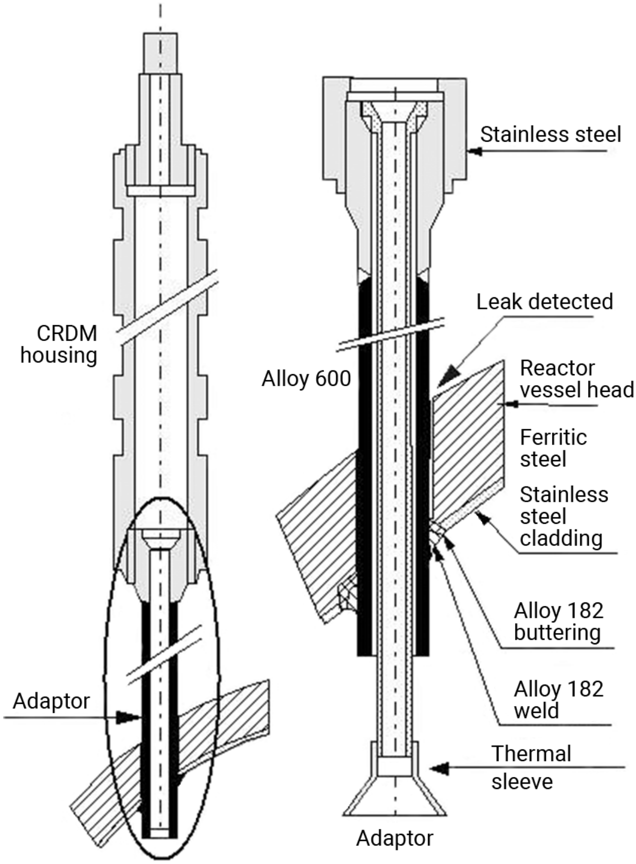


Figure 27.4. Latch housing of a rod cluster control assembly mechanism. The adaptor, about 15 mm thick, is made from alloy 600; the buttering and welding are in alloy 182. IRSN.

Non-destructive tests carried out on the adaptor in question revealed about ten cracks aligned with the adaptor axis (longitudinal defects), measuring up to 8 cm in length.

Investigations then began on all adaptors at this unit and on those of the two units of the same design that were shut down at the time (Fessenheim 1 and Bugey 4). Cracks were identified on these three vessel closure heads. These defects were attributed to stress corrosion in the metal used to make the adaptors, which developed during reactor operation.

The cracking observed could have been linked to the following conditions:

– the vulnerability of alloy 600 to stress corrosion,

– the existence of residual stress due to ovalling of the adaptors when they were welded to the vessel closure head during assembly,

- the temperature under the reactor vessel head when the unit is in operation (about 315°C).

Data on stress corrosion propagation kinetics showed extensive dispersion. At 315°C, depending on the vulnerability of the alloy 600 material used, the propagation velocities were estimated to be between a few tenths of a millimetre and a few millimetres per year.

The vessel head adaptor found to be leaking at Bugey Unit 3 was removed and examined. Metallographic examinations revealed intergranular cracking characteristic of stress corrosion of the alloy 600 material in the reactor coolant environment, with two cracks where the adaptor was welded to the vessel closure head. They began at the base of the weld zone and advanced symmetrically towards the top and bottom of the adaptor. The longest crack emerged at the outer wall of the adaptor and an examination of this area showed that the crack had gradually crossed the adaptor during unit operation and had propagated in the deposited metal of the weld.

The examination also revealed circumferential cracks around the outside of the adaptor. These cracks, which had initiated at the weld root, had propagated in the adaptor base metal and in the deposited metal. They were probably due to the fact that the interstice between the adaptor and the vessel head had been maintained in the presence of reactor coolant as a result of the cracking across the adaptor. The depth of these cracks did not exceed 2 mm in the adaptor and 3.5 mm in the weld. The cracking that propagated in the weld could have started from a 'hot cracking' fabrication defect.

27.2.2.1. Condition of other reactors

The design of the adaptors on other reactors in the fleet in operation at the time was basically the same. Analysis of the parameters that could have had an influence on the stress corrosion of these adaptors initially led to the following classification of the different French reactor series based on this damage risk:

- the six reactors of the Fessenheim and Bugey nuclear power plants started up between 1977 and 1979: in these reactors, the temperature under the closure head during operation is approximately 315°C;
- the other 900 MWe reactors (28 reactors): the temperature under the closure head in these reactors is only about 290°C;
- the 20 reactors in the 1300 MWe series, started up between 1984 and 1992: the temperature under the closure head of some of these reactors was higher (between 315°C and 320°C).

The French Nuclear Installations Safety Directorate nevertheless requested surveys of all the reactor types.

In November 1992, cracks were found in three of the 65 adaptors at Blayais Unit 1 (900 MWe reactor), showing that the anomaly could affect all the reactors in the

French nuclear power plant fleet. This led to the definition of an extensive inspection programme covering each type of reactor. To begin with, these inspections were carried out using manual methods requiring the dismantling of the control rod drive mechanisms and thermal sleeves, but later on they were carried out using robot systems to limit the dismantling required and the exposure of personnel to radiation.

Generally, the cracks detected affected only peripheral adaptors, but they could be found on all reactor types. The vents[728] in the vessel closure heads were not found to have cracks, even though they were originally thought by EDF to be precursors to the adaptor cracking[729].

It became apparent that the temperature under the vessel closure head was not a decisive factor in the occurrence and development of stress corrosion in adaptors – studies and research conducted on stress corrosion of nickel-based alloys subsequently confirmed that, although temperature plays a role, other factors related to the material and its manufacturing process also play a decisive and possibly greater role.

27.2.2.2. Impact on safety

The longitudinal defects observed were not likely to negatively affect the mechanical strength of the adaptors in the absence of a leak. However, a borated coolant leak could cause corrosion of ferritic steel in the closure head.

In the specific case of the adaptors, corrosion of the ferritic steel could even be accelerated by a concentration of boric acid in the interstice between the adaptor and the closure head, through evaporation of the coolant. In the absence of any evidence to the contrary, it seemed prudent to try to avoid any leaks from an adaptor. This position was backed up by findings related to the penetration examined at Bugey Unit 3, which revealed the possibility of circumferential cracks from the outside surface, the development of which could be accelerated by the presence of concentrated boric acid.

In keeping with the defence in depth principle, the most severe conceivable accident was studied: this was the rupture of an adaptor leading in particular to ejection of the associated (control) rod assembly and to depressurization of the reactor coolant system.

The control rod ejection accident studied in the safety analysis reports corresponds to a reactivity insertion accident leading to a sudden increase in reactor power (see Chapter 35). The selected initiating event is ejection of the plug from a rod cluster control assembly travel housing (40.6 mm diameter), but the pressure decrease induced by the break is not taken into account when assessing the maximum pressure reached in the reactor coolant system, which is calculated taking into account only the heating

[728] Vents are small tubes that pass through the closure head to vent the vessel when the reactor is being started up or restarted. They are then plugged.

[729] A leak from a vent (made from alloy 600) occurred in 2010 at Unit 3 of the Korean Yong-Gwang nuclear power plant.

of the water due to the power excursion; this is obviously pessimistic. The maximum value obtained is 190 bars, which is much lower than the hydrotest pressure.

It was shown that, in the event of an adaptor rupture and taking into account the break caused by ejection of the whole mechanism (101.6 mm diameter), the maximum pressure reached would be below that of the case studied in the safety analysis reports. The calculations also showed that, in the event of an adaptor ejection, the forces on the RCCA guides and the upper core plate would be well below the loads used as the design basis. This type of accident must nonetheless remain an exceptional event.

It could not be demonstrated, however, that adaptor ejection would not lead to the rupture of a neighbouring adaptor affected by defects. The simultaneous ejection of two shutdown rod cluster control assemblies that were initially fully inserted (contrary to the operational limits and conditions) would lead to fuel damage. Particular precautions were therefore required.

27.2.2.3. Prevention, monitoring and mitigation

Various measures were therefore taken to improve crack prevention, ensure cracks were detected in good time and mitigate any consequences.

A modification was made from early 1992, during annual outages, to lower the temperature under the vessel closure heads of all 1300 MWe reactors to about 290°C. This measure was implemented despite the discovery of defects in 900 MWe reactors (where the temperature under the vessel closure head is 290°C) because it would be beneficial in any case – even though temperature is not the only influencing factor.

27.2.2.4. Developing inspection tools

Automated means of inspection were developed to increase the potential to inspect adaptors while reducing the radiation doses received by the personnel concerned. The techniques used were eddy current examination and ultrasonic examination, as well as video inspection and liquid penetration testing:

- the facility operator had two devices available for video inspection: one could be used to examine the outer surface of the closure head to detect any traces of boron; the other to examine the inner surface of the closure head to detect any cracks either in the welds between the adaptor and the vessel closure head, or on the inner face of the adaptors, where they were not fitted with thermal sleeves;
- a device for remote liquid penetrant testing was developed as a complement to video inspections; when used to inspect several welds on the closure heads of units 3 and 4 at the Bugey nuclear power plant, it did not reveal any signs of cracking;
- from 1992 onwards, the operator was equipped with automated non-destructive test methods that did not require removal of the thermal sleeves. These methods use contact eddy current testing, which can detect longitudinal

or circumferential cracks in the weld zone; the probe is inserted into the adaptor between the thermal sleeve and the adaptor itself. The depth of any defects is then determined by ultrasonic inspection of the cracks detected in the weld zone, which requires removal of the thermal sleeve.

The operator was therefore able to implement an inspection programme to gain a better idea of the extent of the problem and how quickly it was evolving.

Based on the results, it could be considered that a progression of 4 mm per cycle was sufficiently bounding to cover measurement inaccuracy.

27.2.2.5. Repairs

In addition to the cracked adaptor at Bugey Unit 3, which was replaced using a procedure that took a long time to develop (and which led to significant radiation exposure of the workers involved), the closure heads of the Bugey Unit 4, Paluel Unit 4 and Flamanville Unit 1 were also repaired in 1992.

Analysis of the file submitted by EDF in early 1993 prompted the French Nuclear Installations Safety Directorate, on the advice of the Standing Nuclear Section and the Advisory Committee for Reactors, to issue notification of a criterion for the repair of cracked penetrations. It required the repair of all cracks that were through-wall or likely to become so during the next operating cycle. Although the adaptor thickness is about 15 mm, a crack in the weld zone between the adaptor and the closure head or above this must be repaired when the thickness of sound metal behind the crack is less than 4 mm.

The programme to replace the affected closure heads (see further on) in fact meant that the repair programme remained on a small scale.

27.2.2.6. Leak detection

As it is important to detect leaks quickly, measures were developed for this purpose, based on the detection of nitrogen-13[730]. The corresponding systems were initially set up at the reactors the most affected, then later at reactors where exhaustive adaptor inspections had not yet been carried out.

If water leaks from the reactor coolant system, nitrogen-13 is found under the removable insulation of the closure head (casing), so permanent gas sampling was set up, with a counting channel consisting of two sensors to measure the corresponding radioactivity. This method can detect a leak of less than 1 kg/h.

[730] Nitrogen-13 is produced in the water used to cool the reactor core; its radioactive decay leads to the emission of two types of 511 keV gamma radiation (in opposing directions), with a radioactive half-life of ten min.

27.2.2.7. Anti-ejection devices

Anti-ejection devices were installed at the Fessenheim and Bugey units to prevent the bottom of a broken adaptor from coming out of the vessel head.

Because of the vessel head inspection, repair and replacement programme, it was not considered necessary to ask EDF to fit the other 900 MWe units with anti-ejection devices.

27.2.2.8. Current situation

Because of the cracks found, EDF decided to replace all the vessel heads on reactors in the French nuclear power plant fleet that had adaptors made from alloy 600; these replacements began in 1994 and were completed by the end of the 2000s. They affected all the 900 MWe and 1300 MWe reactors; the 1450 MWe reactors had benefited from this operating experience feedback when they were commissioned, so their vessel heads were fitted with adaptors made from alloy 690.

No stress cracking has been found in adaptors made from alloy 690. The adaptors in some control vessel heads are nevertheless inspected using eddy current testing during complete inspection outages (every ten years).

27.2.2.9. Cracks observed on reactor vessel heads in other countries

One of the most notable events outside of France occurred in 2002 at the Davis-Besse nuclear power plant[731] in the USA (Ohio).

On 5 March 2002, during a refuelling outage, damage to the vessel head was discovered on a rod cluster control assembly adaptor, due to stress corrosion of the nickel-based alloy used for the vessel head penetrations. Investigations revealed a cavity throughout the entire thickness of the carbon steel, such that the reactor coolant system pressure was only contained by the stainless steel cladding (a few millimetres thick), which had an area of swelling and a through-wall crack in the location of the corrosion cavity. The cavity was caused by water leaking from the crack in the adaptor and corrosion by boric acid. The event was considered to be a precursor to an accident; the accident that could have occurred was an ‘intermediate’ size reactor coolant system break in the reactor vessel head, probably with rod cluster control assembly ejection. Scenarios with more serious consequences could also be envisaged, such as ejection of several RCCAs and a large tear in the reactor vessel head[732]. Although the technical causes were identified, particularly the sensitivity of the nickel-based alloy to stress corrosion, causes of an organizational nature were also exposed involving the operator, First Energy Nuclear Operating Corporation (FENOC), and beyond that, safety management and control practices in general.

[731] This nuclear power plant, in the state of Ohio, has a single 837 MWe pressurized water reactor.

[732] This event was rated Level 3 on the INES scale.

Although boric acid deposits on the adaptor concerned had been observed as early as 1998, no corrective action had been taken and video inspections carried out on several occasions had never spotted the cavity developing in the vessel head.

In addition, the first obvious signs of cracking in vessel heads had been discovered in March and April 2001 in units similar to the one at Davis-Besse. A programme to study the vulnerabilities of US reactors was conducted. The results, which were made known in May 2001, showed that Davis-Besse was one of the most vulnerable reactors, but the operator did not carry out inspections until March 2002, during the scheduled refuelling outage.

Generally, the lessons learned from this event confirmed the validity of the measures adopted by EDF with regard to vessel heads on French nuclear power reactors, explained above.

27.2.2.10. Implementation of special monitoring for 'Inconel areas' beginning in 1992

Degradation caused by stress corrosion of alloy 600 parts had first been noticed in steam generator tubes, then in the instrumentation nozzles of pressurizers at 1300 MWe reactors. This type of degradation at the Gravelines nuclear power plant in 1991 led EDF in 1992 to propose to the safety organizations a specific approach and multi-annual monitoring programmes for areas in the main primary system made from alloy 600.

The areas in the main primary system the most vulnerable to stress corrosion were identified based on the intrinsic vulnerability of the material, stresses in steady states (excluding transients) and the operating temperature[733]; in descending order of vulnerability[734], these were:

- peripheral adaptors[735] that accommodate the RCCA drive mechanisms where they pass through the vessel heads,
- divider plate to stub runner welds in steam generator channel heads,
- vessel 'lower head penetrations'[736] that did not undergo stress relieving treatment (which was the case for penetrations that had to be repaired after the vessel underwent stress relieving treatment),

[733] The higher the temperature, the greater the stress corrosion risk.

[734] The vulnerability of steam generator tubes made from alloy 600 was identified in the laboratory, then observed on sites in the 1980s. The tube monitoring programme is specific and separate from the 'Inconel zones' file for historical reasons and because of the specific nature of the inspection methods.

[735] Peripheral adaptors have a high residual stress level because of the specific welding geometry; they also do not benefit from the stress relieving heat treatment applied to vessel heads.

[736] Leaktight devices in the vessel lower head to accommodate passage of the core instrumentation (in-core instrumentation system, ICS).

– reactor vessel clevises ('M supports') in the lower part of the vessel, which provide radial support for the internals.

The monitoring programmes evolved and were reinforced over time to take into account observations and research and development results[737]. Observations concerning vessel lower head penetrations and steam generator tubes will be discussed later.

These programmes were analysed in detail by the safety organizations; the BCCN, IPSN and the Standing Nuclear Section were particularly involved.

In 2001, the French Nuclear Installations Safety Directorate issued a decision[738] setting the conditions for in-service monitoring of areas of Inconel® 600 in reactors. This decision takes into account the most sensitive areas identified, but also requires that inspections be extended to other areas to take into account the difficulty of defining exactly when stress corrosion starts to occur based on the accumulated operating time of the equipment.

27.2.3. Cracking on vessel lower head penetrations detected in 2011

The discovery of characteristics indicating the initiation of stress corrosion cracking in divider plates made using alloy 600 in steam generator channel heads (especially in 2002 in the channel head of steam generator 2 at Chinon Unit B4, where cracking was not expected to have started), showed that the models for predicting time to initiation were subject to significant uncertainty and that these time periods could consequently be overestimated. It was therefore necessary not only to inspect all steam generator channel heads – rather than just carrying out sampling inspections as required by monitoring programmes at the time – but also to extend these inspections to vessel lower head penetrations made from alloy 600, even though these areas had been considered less vulnerable than the steam generator channel heads. A significant event had to be taken into account in this regard: in 2003, leaks had been detected in two vessel lower head penetrations at Unit 1 of the South Texas nuclear power plant in the USA (Texas), after only 15 years of operation (these vessel lower head penetrations had not undergone stress relieving treatment[739]).

The French safety authority therefore asked EDF to carry out non-destructive testing of the vessel lower head penetrations in 900 MWe reactors during their third ten-yearly inspection.

[737] Some of the R&D on stress corrosion of nickel-based alloys is mentioned in Section 10.1 of the book Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

[738] Decision DSIN-BCCN/MP/AR No. 010067 of 5 March 2001.

[739] Stress relieving treatment is a heat treatment designed to reduce (or relax) the stresses induced by fabrication, especially welding.

Thus in October 2011, indications of longitudinal cracking were detected in vessel lower head penetration 4 of Gravelines Unit 1 (900 MWe) during ultrasonic testing of the vessel lower head penetrations as part of its third ten-yearly inspection (see Figure 27.5). These indications were detected in the corner weld connecting the vessel lower head penetration to the inner surface of the vessel. They were nearly as deep as the thickness of the vessel lower head penetration. The defect was considered to be a through-wall crack in the base metal directly under the weld; however, further examinations revealed that there was no leakage path, and no leaks were detected.

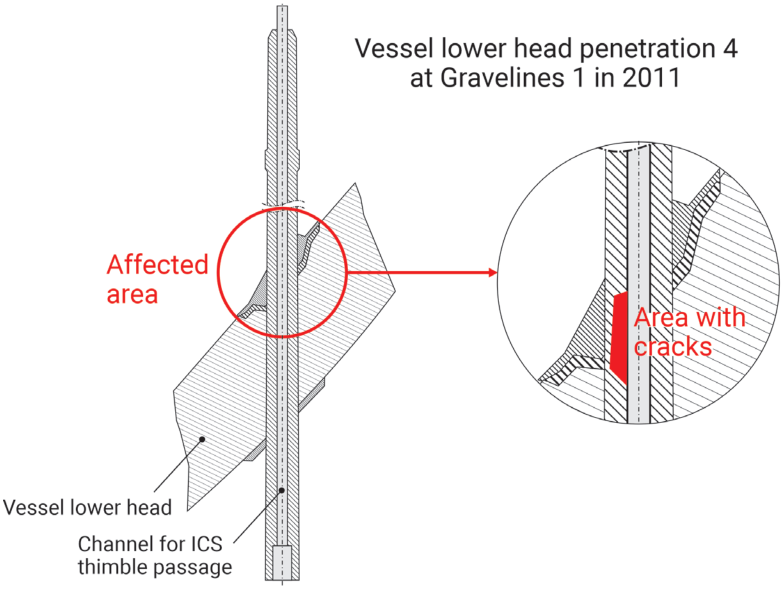


Figure 27.5. Unit 1 at the Gravelines nuclear power plant: diagrams of vessel lower head penetration 4 and the area with cracks. IRSN.

The affected unit had been commissioned in 1980 and inspections conducted in 2001 had revealed no indications of stress corrosion cracking. Only two indications of longitudinal cracking in this area, attributed to metallurgical heterogeneities dating from fabrication, were identified. The vessel lower head penetrations in Unit 1 at the Gravelines nuclear power plant had been welded before the final stress relieving heat treatment of the vessel was carried out.

Until then, the sensitivity of alloy 600 to stress corrosion had appeared to affect only components exposed to hot-leg temperature conditions without having undergone stress relieving heat treatment. This incident showed that stress corrosion cracking could appear in service under cold-leg temperature conditions and in areas that had undergone stress relieving heat treatment. Maintenance programmes now take into account this risk.

One consequence of this degradation could be corrosion of the vessel wall, leading to a leak at the vessel lower head that cannot be isolated.

27.2.4. Monitoring the 'beltline' region of the vessel

The beltline region of the vessel is the part of the vessel's cylindrical shell that is exposed to radiation from the core. This exposure can weaken the steel that the vessel is made of by changing its mechanical properties, leading particularly to embrittlement. Embrittlement is manifested by an increase in the ductile-brittle transition temperature, which adversely affects the material's ability to withstand a cold thermal shock[740]. Embrittlement is assessed (and predicted) using empirical models adjusted to data from the analysis of test specimens from the irradiation monitoring programme, in addition to irradiation programmes conducted in experimental reactors[741].

The irradiation monitoring program involves testing samples, for each vessel in the French reactor fleet, representative of the steel that the vessel is made of, placed inside capsules around the circumference of the reactor core. These capsules also contain dosimeters to measure the neutron fluence received by the samples. Due to their location, the capsules are exposed to a higher neutron flux than the vessel. This makes it possible to predict the behaviour of the materials after 10, 20, 30 or 40 years of operation, or even longer.

In-service inspections are also carried out on the vessel beltline region using machines specifically developed and improved over time (in-service inspection machines – see Figure 27.6).

The analysis of vessel fitness-for-service, carried out by the operator during the periodic reviews associated with the ten-yearly reactor outage, includes an analysis of fast fracture risk. This analysis aims to study the risk of initiating postulated defects, where defect geometry and dimensions are defined conventionally (i.e. depth is one quarter of the vessel wall thickness). The mechanical properties considered for steel take into account the irradiation received, and the load applied is the load that would result from the worst-case thermal transients (for example, an influx of 'cold' water from the safety injection system if there was a break in the reactor coolant system[742]). If a real defect is detected, it must be demonstrated that it will not constitute a fast fracture risk during thermal transients of this type.

[740] A sudden influx of water at a lower temperature than the water initially present in or near the structure (such as a reactor vessel).

[741] Several programmes are mentioned in Section 10.1 of the book Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

[742] Thermal transients cause complex flows in the vessel. Tests are carried out on mock-ups and loops to provide knowledge that sometimes cannot be obtained using numerical simulation or may be subject to significant uncertainty.

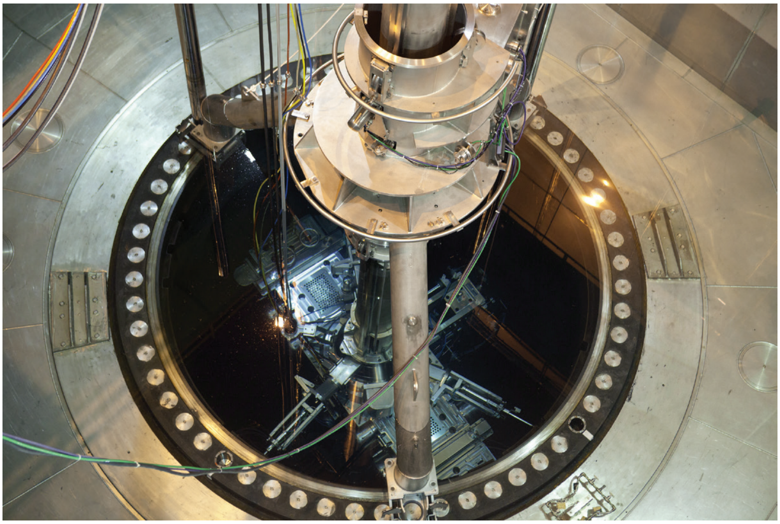


Figure 27.6. A machine for in-service inspection of a pressurized water reactor vessel at the Bugey nuclear power plant. Bruno Conty/EDF.

27.2.5. Defects observed on reactor vessels in Belgium

In June 2012, inspections were carried out on the vessel of Unit 3 at the Doel nuclear power plant. For the first time in Belgium, the entire inner surface of the vessel beltline region was inspected using ultrasonic examination. These inspections aimed to find any underclad defects, as is the practice in France. The inspections revealed indications that the operator believed were due to defects in the steel that the vessel was made of (see Figure 27.7). Many of these indications, which were oriented more or less in parallel to the vessel's inner wall, were 12 to 16 mm in length.

In September 2012, an ultrasonic examination was conducted on the vessel of Unit 2 at the Tihange nuclear power plant, fabricated by the same Dutch company, RDM[743]. Inspection of the Tihange Unit 2 vessel led to detection of defects similar to those found in the Doel Unit 3 vessel.

Both of these findings and the location of the indications suggested that they were due to hydrogen-induced flaws; they could have been caused by hydrogen present in the metal during fabrication by the Dutch company RDM. It can be the case that, when steel parts are being fabricated, the hydrogen concentration in the steel when it is cooled and hardened is too high; this can lead to hydrogen-induced flaws (fine decohesion) in the steel of the forged parts.

As a result of this discovery, the Belgian safety regulator (AFCN) decided that neither of the units affected by these defects could be restarted until the operator,

[743] Rotterdamsche Droogdokmaatschappij (RDM).

Electrabel, had demonstrated that the presence of hydrogen-induced flaws had no impact on vessel integrity and therefore vessel safety.

The technical investigation of this case, which involved Electrabel, the Belgian organizations AIB-Vinçotte and Bel V, and also Oak Ridge National Laboratory[744], was not closed until three years later, once samples representative of the mechanical strength of the vessels had been tested and analysis results had shown that the observed defects were not a source of risk. Authorization to restart Doel Unit 3 and Tihange Unit 2 was eventually granted by AFCN in November 2015.

The Dutch company RDM, which is no longer in existence, did not fabricate vessel shells for any French nuclear power plants.

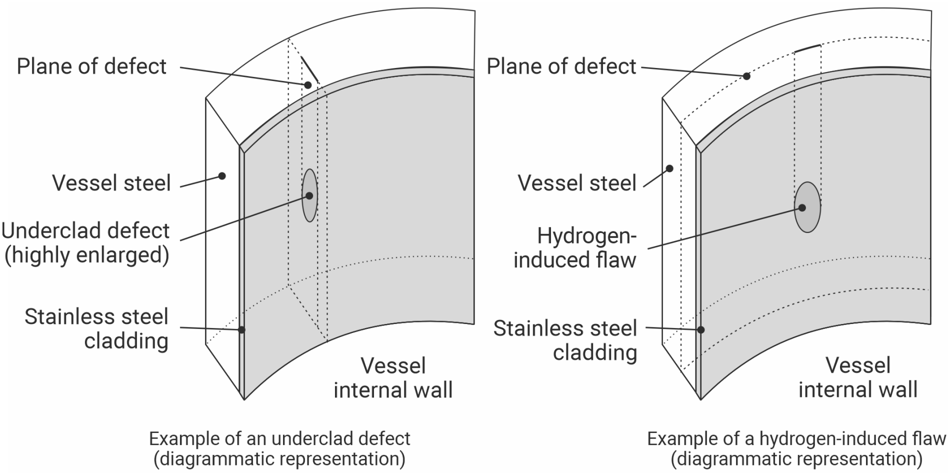


Figure 27.7. Diagrams showing underclad defects (left) and hydrogen-induced flaws (right) found in Unit 3 at the Doel nuclear power plant in Belgium. IRSN.

Hydrogen-induced flaws are generally associated with segregation zones. They appear as multiple microcracks oriented more or less in parallel to the internal wall of the vessel. To prevent these defects, the hydrogen concentration is controlled during casting and a special heat treatment is applied during forging to minimize hydrogen concentration in the metal. In the last 50 years, only a few parts built for the French nuclear power plant fleet have presented hydrogen-induced flaws and have been discarded following inspections by the manufacturer.

An investigation was conducted by EDF and the manufacturer of French vessels based on the fabrication documents. The results of this research did not lead to suspicions that large numbers of hydrogen-induced flaws might be present, because of the fabrication measures and inspections implemented for vessels in the French nuclear power plant fleet. Reviews of inspections carried out during complete inspection

[744] As well as experts from ASN, IRSN, GRS, etc.

outages and specific inspections to detect hydrogen-induced flaws were carried out by EDF: no defects comparable to the hydrogen-induced flaws detected in the Belgian Doel Unit 3 and Tihange Unit 2 vessels were found.

27.3. Steam generators

The importance of having steam generator tubes that perform correctly to ensure safe facility operation and prevent radioactive release into the environment has been highlighted several times in previous chapters. These components are therefore naturally the focus of ongoing attention.

For the operator, this consists in identifying the different types of defects that can affect the tubes, assessing the associated rupture risks, and defining and implementing monitoring programmes and preventive measures such as plugging tubes affected by defects.

27.3.1. The different types of defects

Experience gathered worldwide shows that steam generator tubes can present a wide variety of defects resulting from different mechanical or physical-chemical phenomena (see Figure 27.8). These types of defects have appeared over time, sometimes after relatively short operating periods.

The first type, known from US experience, is constriction of the tubes at the tube support plates (known as 'denting'). The other types can be classified based on the phenomenon involved, which may affect only certain units. In particular:

– cracks in alloy 600 caused by stress corrosion from the reactor coolant system water:
    - in small U-bend tubes in 900 MWe units,
    - in roll transition zones[745];

– alloy 600 corrosion from the secondary system water:
    - intergranular corrosion (IGC) at the tube support plates in the case of alloy 600 MA,
    - intergranular corrosion at tube ends,
    - circumferential stress corrosion cracking at tube ends,

[745] Rolling consists of enlarging the part of a steam generator tube inserted into the tubesheet to make sure there is continuous contact between the tube and the tubesheet; this avoids crevices, which can be the site of major corrosion. The tube is then welded at the channel head end. Several techniques have been used successively to limit the induced stresses.

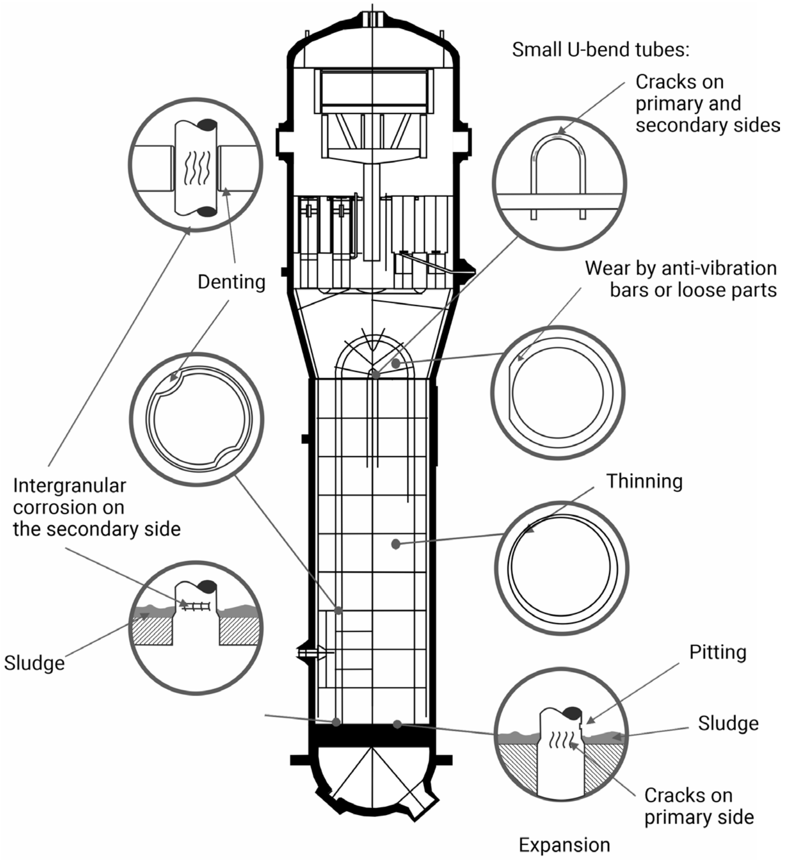

Small U-bend tubes:
Cracks on primary and secondary sides
Wear by anti-vibration bars or loose parts
Thinning
Pitting
Sludge
Cracks on primary side
Expansion
Denting
Intergranular corrosion on the secondary side
Sludge

Figure 27.8. A few types of steam generator defects. Georges Goué/IRSN.

- wear on the secondary side:
  - from loose parts,
  - from contact between the tubes and anti-vibration bars,
  - from contact between large U-bend tubes,
- other deformations at the tube support plates.

Other phenomena have appeared on reactors in other countries. This is the case with vibration fatigue[746], which led to complete guillotine breaks in tubes at the North Anna nuclear power plant in the USA (in 1987) and at the Mihama nuclear

[746] Fatigue due to the vibratory environment. It is related to the interaction between a fluid and a structure, the presence of turbulence and a phenomenon referred to by specialists as 'fluid-elastic whirling'.

power plant in Japan (in 1991). Phenomena attributed to vibration fatigue also appeared in France between 2004 and 2006, but were detected before a complete steam generator tube break[747] occurred. This subject will be covered in further detail in Section 27.3.7.

Concerning tube corrosion risk, all steam generators installed since 1992 in the nuclear power plant fleet (replacement steam generators and generators in new units) have been fitted with alloy 690 TT tubes, which exhibit satisfactory behaviour in operation and to date have not shown any signs of corrosion.

27.3.2. Associated risks

The risks associated with steam generator tube degradation are obviously the rupture of one or more tubes, in normal operation or in an accident situation (steam-line break). These breaks are taken into account as accidents in the design and safety demonstration of nuclear power reactors. However, in accordance with the defence in depth concept, the risk of steam generator tube rupture must be carefully limited, particularly because this type of rupture could lead to release of radioactive substances outside the facility.

In normal operation, the tubes are subject to a pressure differential of about 100 bars. But in an accident situation, such as a sudden pressure drop in the secondary system caused by a water-line or steam-line break, the situation must not be aggravated by the rupture of one or more steam generator tubes; if it is, the pressure differential between the two tube faces is about 172 bars and this mechanical load must be combined with the dynamic effect of depressurization (and by convention, for the safety demonstration, with the seismic margin earthquake).

Some events, like the event in 1984 at Unit 5 of the Bugey nuclear power plant involving the failure of three out of four electrical power sources, have actually led to steam generator tubes being subjected to high pressure differences, though not as high as the level mentioned above.

Analysis distinguishes between two types of defect: those for which it can be demonstrated that there will be a detectable leak before the risk of rupture and those for which this cannot be demonstrated. In the first case, the facility can be shut down before a defect becomes unstable and risks causing leakage of radioactive substances – monitoring and detection of leaks between the reactor coolant system and the secondary system is therefore essential; in the second case, the possibility of an instantaneous fast fracture must be considered – only preventive monitoring efforts combined with plugging the affected tubes will be effective (see Figure 27.9).

[747] The leak rate reached 400 L/h in 2006 at Unit 4 of the Cruas-Meysse nuclear power plant, just below the rate that could lead to a complete tube break.

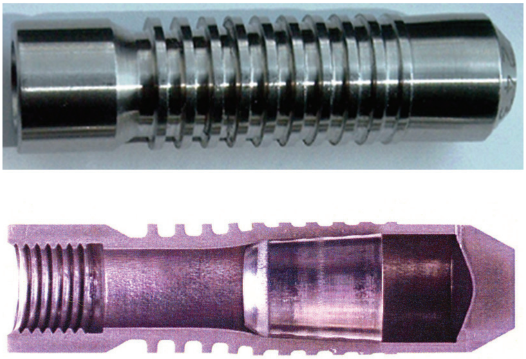


Figure 27.9. View of a current model of steam generator tube plug. Photo from *La maintenance des centrales nucléaires* (Maintenance at Nuclear Power Plants) by Jean-Pierre Hutin – EDF/Lavoisier Tec&Doc, 2016.

27.3.3. Monitoring during operation and inspection during outages

27.3.3.1. Monitoring during operation

Continuous monitoring of steam generator tubes during unit operation is accomplished using two methods: noise measurement, to detect loose parts, and measurement of leakage between the reactor coolant system and the secondary system.

At the time the French units went into operation, the operational limits and conditions required units to be shut down as soon as the leak rate from the reactor coolant system to the secondary system exceeded 70 L/h, which was the value set by US operators; this threshold was designed to limit contamination of the secondary system water.

It was only after the first tube defects were detected that the link between leakage and rupture risk was researched. As analyses progressed and experience was acquired, the French safety organizations asked EDF to reduce the tolerated leak rates, in view of the sensitivity of the means of detection and the location of the tubes that had presented or could present defects.

The following means of detection are used:

- measurement of radioactivity in the gases extracted from the condenser,
- measurement of radioactivity in the water inside the blowdown system of each steam generator,
- measurement of radioactivity from nitrogen-16 in the secondary system fluid using a device installed in each steam generator steam line.

Leak detection between the reactor coolant system and the secondary system by measuring nitrogen-16 radioactivity through the secondary system piping is the quickest method and one of the most sensitive. Leakage of approximately 3 to 5 L/h can be detected almost instantly and with satisfactory accuracy; this is 20 times less than the limits initially allowed.

27.3.3.2. Inspection during reactor outages

All steam generator tubes are inspected along their entire length using an axial eddy current probe before each unit is started up and the recordings are archived. The roll transition zone is also inspected using a rotating eddy current probe.

In-service monitoring is performed by inspecting, during one out of two refuelling outages, any tubes in which defects have previously been detected and left untreated, as well as a sample of tubes to detect the extent of any degradation developing gradually or any new types of defects. The basic sampling rate for each steam generator at each outage, on average, is:

- for 900 MWe units equipped with alloy 600 TT and 690 TT tubes: 1 tube out of 8 (all tubes have therefore been inspected by the end of eight operating cycles);
- for 1300 MWe units equipped with alloy 600 TT tubes: 1 tube out of 6 (all tubes have therefore been inspected by the end of six operating cycles);
- for 1300 MWe and 1450 MWe units equipped with alloy 690 TT tubes: 1 tube out of 8 (all tubes have therefore been inspected by the end of eight operating cycles).

To ensure all steam generator tubes in a reactor have been inspected by the end of six or eight operating cycles, sampling inspections are obviously carried out on different tubes at each inspection. Detection of a particular type of defect can lead to an increase in the sampling rate or the inspection of all tubes in a particular area.

This practice naturally has very little chance of detecting an isolated defect with rapid kinetics, which explains the importance of detecting loose parts.

During the ten-yearly reactor outages, all the tubes are inspected again.

27.3.4. Steps to be taken when a defect is detected

When a defect is detected, the following approach is used to determine which measures should be taken:

- determination of the causes of the degradation,
- assessment of the risks of instability that could be caused by the defect in a normal or accident situation, potentially leading to a rupture not preceded by leakage,
- assessment of the ability of monitoring methods to detect and characterize the degradation,

- adjustment of the scope and frequency of inspections in order to prevent tube ruptures,
- plugging the tubes, if the criteria justifying this action are met.

A few examples illustrate this approach.

27.3.4.1. Tube wear due to foreign matter

Where there is uniform wear of a tube along a length of several centimetres, the risk of a rupture not preceded by a leak cannot be ruled out. Tube ruptures that have occurred in the USA confirm this (Prairie Island in 1979, Ginna in 1982[748]).

An axial probe is generally capable of detecting these defects, but the depth of wear can be difficult to assess accurately.

Monitoring consists of a detailed visual inspection of the perimeter of the tube bundle during each unit outage. When an object likely to cause wear is observed, all tubes around the perimeter of the tube bundle are examined using the axial probe. Tubes showing wear of more than 40% of their thickness are plugged.

Extraction of any detected loose part is always attempted. If it is stuck and cannot be removed, all tubes likely to come into contact with it are plugged, even if they show no signs of wear.

27.3.4.2. Wear due to contact with anti-vibration bars

The length of tube wear due to friction with anti-vibration bars is limited to the thickness of the bars. It is possible, in this case, to show that any perforations affecting the tubes are stable, including in accident conditions. There is therefore no risk of fast fracture of a tube as a result of this type of wear.

The axial probe can detect this type of defect and the depth of wear of the tubes can be determined by interpreting the signals, by means of tests and numerical simulations that have been carried out.

Monitoring covers the tubes in areas of the steam generators where these phenomena have been observed, generally after at least six years of operation.

Tubes in which wear has reached more than 40% of the tube thickness are plugged, which takes into account:

- wear rates that could lead the defects to open up,
- the wear kinetics observed,
- the period between inspections.

[748] Leaks and tube perforations due to loose parts (caused by wear) have occurred since, but no clean breaks.

Every tube that has given a wear signal and has been left untreated is inspected after two further operating cycles.

27.3.4.3. Cracking in U-bend tubes

This type of degradation, attributed to stress corrosion, affected certain tubes in the first and second rows in some steam generators at the oldest 900 MWe units with alloy 600 MA tubes. This damage affected the tubes with the smallest bend radius, which had not undergone stress relieving treatment after they were bent in the factory and were not subject to heat treatment on site. The actual morphology of the defects was difficult to predict. Moreover, it could not be guaranteed that a detectable leak would precede rupture. Research and development work is under way on this topic for alloy 600 TT tubes.

The helium leak tests carried out during the ten-yearly outage[749] obviously only detect through-wall cracks. Furthermore, when the axial eddy current testing probe passes through small, tightly bent U-bend tubes, it can shift off-centre, reducing its detection sensitivity.

Two measures were taken by EDF:

- preventively plugging the tubes in the first row or the first two rows;
- or stress-relieving heat treatment; after this treatment, the U-bends were inspected again using the axial probe at each refuelling outage; no new defects were detected in the treated tubes.

All steam generators in the French nuclear power plant fleet with alloy 600 MA tubes have been replaced.

27.3.4.4. Tube deformation and cracking

A leak from a steam generator tube appeared during the first operating cycle at Unit 1 of the Nogent-sur-Seine nuclear power plant (a 1300 MWe reactor commissioned in 1988). The inspections carried out revealed a new type of degradation affecting only the 1300 MWe units[750].

This type of degradation was attributed to the presence of iron-based metal residues from grinding or shot-blasting operations, which had collected in the centre of the tubesheet after circulation of the secondary system water had been established. These particles had oxidized with the increase in temperature and then aggregated. The ‘swelling’ had caused deformation of the tubes in the roll transition zone that could have led to circumferential cracking of tubes through stress corrosion in the reactor coolant environment.

This new phenomenon prompted EDF to conduct a major investigation programme:

[749] Helium tests are also used to identify any tubes with leaks when an overall flaw signal has been detected.

[750] The steam generator tubes on N4 series reactors are made from alloy 690 TT.

- examination of deposits in the secondary side of the steam generators, determination of their location, height and composition,
- specific examination of the tubes surrounded by deposits,
- tests to reproduce the phenomenon in a laboratory and determine the 'swelling' kinetics of the deposits,
- cleaning of the affected tubesheets,
- plugging any tubes presenting significant deformation, even if there is no sign of cracks,
- reduction of the limit for primary-to-secondary leaks leading to reactor shutdown (3 L/h for alloy 690 TT tubes, 5 L/h for alloy 600 TT tubes).

Experience has confirmed the results of the laboratory tests, which showed that the deposits swell rapidly but only for a few months, i.e. during the first operating cycle.

27.3.5. Steam generator replacement

Steam generator design and fabrication gradually improved, even between the first and last 900 MWe reactors. In particular, the holes in tube support plates are no longer round and drilled but quatrefoil-shaped and broached. These plates are now made from chromium steel. A divider plate has been added to increase the velocity of the secondary system fluid at the centre of the steam generator and thus reduce deposits of oxidation products from the secondary system, mainly magnetite.

The steam generator replacement strategy is focused on:

- mitigating the risk of steam generator tube rupture,
- reducing radiation exposure for personnel who carry out frequent inspections on the most affected steam generators,
- improving operating conditions at reactors where large numbers of tubes have been plugged,
- complying with the safety analysis report, particularly the maximum plugging rate (steam generators must have a minimum heat exchange capacity in order to cool the core in normal or accident operation).

This strategy also takes into account long-term economic and operating considerations.

Obviously, the replacement steam generators have been enhanced, particularly those described above. The tubes of these steam generators are made of alloy 690 instead of alloy 600. The industrial experience feedback for this material is satisfactory; no indications of corrosion have been observed in operation. However, laboratory studies show that it can be vulnerable to stress corrosion in a secondary system environment, particularly in the presence of contaminants such as lead or sulphates.

High-quality conditioning[751] of the secondary system steam generator parts is therefore still necessary.

The first steam generator replacements (see Figure 27.10) were carried out in 1990 at Unit 1 of the Dampierre-en-Burly nuclear power plant. Then the steam generators at Unit 5 of the Bugey nuclear power plant were replaced in 1993, followed by those at Unit 1 of the Gravelines nuclear power plant in 1994. The experience gained made it possible to significantly reduce the accumulated dose received during this work. The collective doses were 2.2 man-Sieverts, 1.5 man-Sieverts and 1.4 man-Sieverts respectively – for just the first three steam generator replacements.

The Gravelines operation was designed and prepared as a standard operation, reproducible with minor adaptations for subsequent replacements, which were carried out at the rate of approximately two per year.

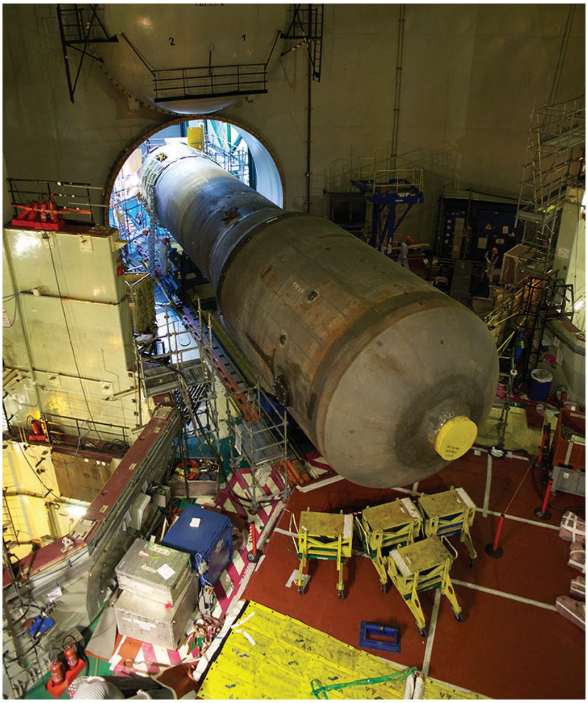


Figure 27.10. New steam generator being moved into a reactor building through the equipment hatch. Jean-Marie Huron/Signatures/IRSN Media Library.

27.3.6. Clogging observed in the 2000s

The Cruas-Meysse nuclear power plant, with four 900 MWe reactors, experienced three unscheduled outages involving major water leakage between the reactor

[751] Raising the temperature by passing steam through these parts.

coolant system and the secondary system at Unit 1 (February 2004) and Unit 4 (November 2005 and February 2006). Investigations conducted by EDF found that fluid-elastic whirling (due to fluid-structure interaction) was the most likely cause of cracks in tubes observed on the top tube support plate (no. 8) of the steam generators. EDF also suspected that the presence of deposits in the quatrefoil-shaped holes that the water passes through (see Figure 27.11) was the cause of this phenomenon, because these deposits could alter the flow on the secondary side of the steam generators, encouraging vibratory instabilities in unsupported U-bends in the central zone of the steam generators, which had tubeless leaf-shaped holes[752].

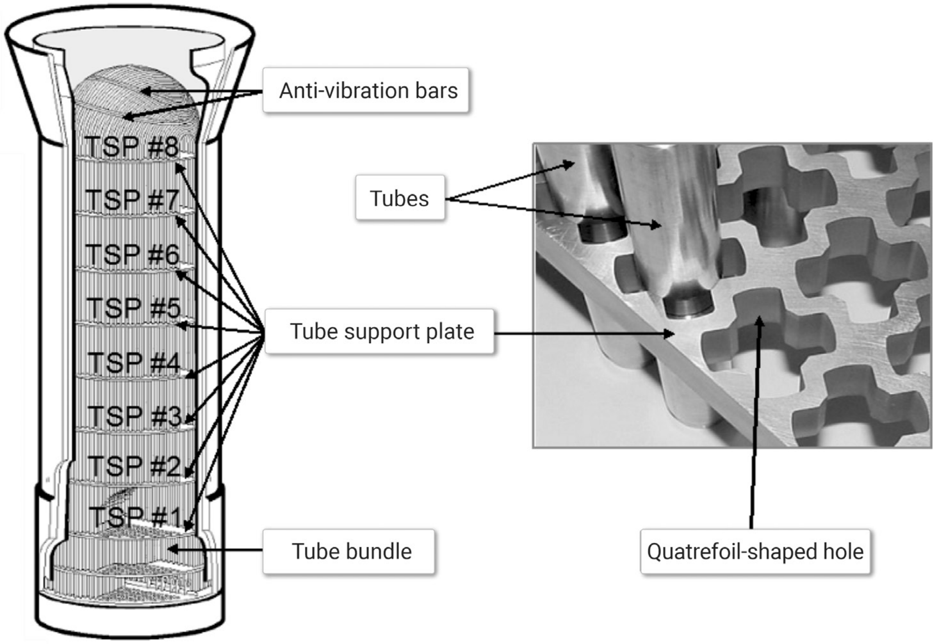


Figure 27.11. Diagram and view showing the tube support plates of the steam generators and the quatrefoil-shaped holes for water to pass through on the secondary side. IRSN.

Video inspections showed that the holes for the water to pass through were about 70% blocked by magnetite deposits, with some even completely blocked.

EDF began studies to understand the phenomena causing the observed cracks and to characterize their consequences for safety. To be able to operate the reactors while limiting the risk of a steam generator tube rupture, as a preventive measure it plugged 58 tubes vulnerable to vibration fatigue in the centre of the tube support plates in

[752] A specific feature of the type of steam generator installed at the Cruas-Meysse nuclear power plant (model 51B).

some steam generators that were significantly affected by clogging. In-service monitoring of leakage from the reactor coolant system to the secondary system was also stepped up.

However, the French safety authority asked EDF to carry out thorough cleaning of the tube support plates in order to restore the steam generators to operating conditions compliant with the assumptions used in design and the safety demonstration. In 2007 and 2008, EDF therefore carried out high-temperature chemical cleaning of the steam generators at units 1 and 4 of the Cruas-Meysse nuclear power plant and Unit 2 at the Chinon B nuclear power plant, and also of the steam generators at Belleville-sur-Loire Unit 1, Cattenom Unit 1 and Saint-Alban Unit 1 (1300 MWe reactors), which were of a different type[753].

Video inspections of all the steam generators in the French nuclear power plant fleet are now carried out (including the N4 series of reactors); cleaning is scheduled to prevent clogging.

27.3.7. Conclusion

No clean breaks of steam generator tubes have occurred in France despite many active degradation mechanisms and a significant number of leaks from the reactor coolant system to the secondary system.

The conclusion should not be drawn from this that breaks are always preceded by leaks; it is important to note in particular that no damaged tubes have ever been subject to the stresses produced by an accident situation such as a steam-line break.

In the mid-1990s, the average frequency of steam generator tube ruptures observed around the world was a few 10^{-3} of major ruptures per reactor year. The measures taken by EDF to manage problems have contributed to the results observed in France. On a worldwide scale, the steam generator tube rupture (SGTR) rate has fallen since then, thanks to the sharing of experience and to measures taken as a result: in 2016, the rate was estimated to be about 5×10^{-4} per reactor year[754].

27.4. Steam lines

From 1990, steam line inspections (see Figure 27.12) revealed traces of cracks in some main steam line welds. These defects were discovered at valve takeoffs on pipes in 900 MWe reactors and some 1300 MWe units.

At the reactors of the Fessenheim and Bugey nuclear power plants, mainly cracking of the steel in the immediate vicinity of the welds was found. The defects were caused by welding operations and were due to insufficient quality of the materials used to

[753] Type 68/19 steam generators.

[754] No SGTRs in France, nine at reactors in other countries.

build the secondary system. ‘Lamellar tearing’ type cracking had spread into the steel from numerous inclusions in the base metal, which were rolled during manufacture. The original pipes in these units were fabricated using the ‘rolled and welded’ technique.

One particular large defect (11 cm in length and 3.5 cm deep along the weld on the takeoff side) was discovered in 1991 at Unit 1 of the Fessenheim nuclear power plant. This defect was not attributed to mechanical fatigue or corrosion, but to a single major case of stress when the pipe was cold during maintenance, which increased the size of one or more small pre-existing defects; this assumption could not be confirmed.

At the other 900 MWe reactors, cracks several millimetres deep and several tens of centimetres long were found on the inner surface at the weld root. This was cold cracking, probably due to poorly controlled welding conditions.

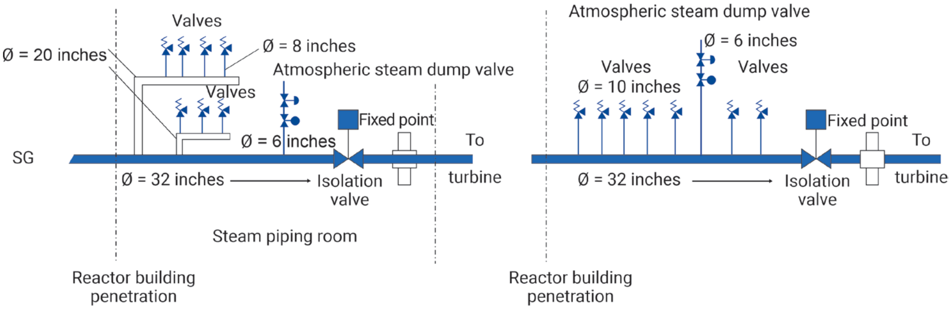


Figure 27.12. Secondary systems at 900 MWe reactors (left) and 1300 MWe reactors (right). IRSN.

In the first generation of 1300 MWe reactors (type P4), welding defects such as inclusions and incomplete fusion, as well as hot cracking, were found; they were mainly due to poorly controlled welding conditions (use of copper nozzles on the welding machine, leading to cracks due to the copper). This was not lamellar tearing because the main pipes had been forged.

The analyses and assessment carried out showed that the defects found, with the exception of the largest one at Fessenheim Unit 1, probably dated from the fabrication of the pipes but had not been detected before startup at the relevant units.

It was the improved inspections demanded by the safety organizations and better operator training that had led to their detection.

Inspections were also carried out on the pipes in the main and emergency feedwater systems.

Defects with dimensions greater than the acceptability criteria were repaired or the affected section was replaced.

27.5. Auxiliary systems: cracks induced by local thermal-hydraulic phenomena

27.5.1. Cracking in non-isolatable sections connected to the reactor coolant loops

Events that occurred in December 1987 at Unit 2 of the Farley nuclear power plant (USA), in June 1988 at Unit 1 of the Genkai nuclear power plant (Japan) and Unit 1 of the Tihange nuclear power plant (Belgium) showed a common factor: leaks and cracks were observed in non-isolatable auxiliary sections of pipe, made from austenitic stainless steel, in the main primary system. In France these events led to a complete fleet-wide study of the 'Farley-Tihange phenomenon[755]' or thermal fatigue cracking of non-isolatable sections in the main primary system. Four years later, however, in September 1992, a similar event occurred at Unit 2 of the Dampierre-en-Burly nuclear power plant, then in December 1996 at Unit 1 of the same plant.

In the case of Farley Unit 2, the leak was in the safety injection system (SIS) line connected to one of the cold legs of the main primary system. At Tihange Unit1, the leak was in a line connected to a hot leg. At Genkai Unit 1, the leak was in a residual heat removal system (RHRS) line.

At Dampierre Unit 2, the leak was in a section of the SIS; the leak rate of the reactor coolant system water, which collected in the containment sumps, was approximately 600 L/h. In the case of Dampierre Unit 1, the leak was also in a section of the SIS, but the leak rate was 160 L/h.

All the cracks were at a weld connecting a section to an elbow, at the bottom of the inside pipe wall.

The cracks were attributed to a thermal fatigue phenomenon in the transition zones where the front of reactor coolant that had entered the auxiliary pipe met a cold water front due to a (small) unintended flow of water from the auxiliary system, caused by an isolation device upstream of the system that was not completely leak-tight. Figure 27.13 shows a diagram of the thermal-hydraulic mechanisms involved.

The thermal fatigue mechanism can be summarized as follows: materials expand and contract cyclically due to the effect of temperature variations, but if they cannot do so freely, stresses occur, which are also cyclical. If these are repeated a large number of times[756], thermal fatigue damage can occur.

[755] Also known as the 'dead leg' phenomenon. Other local thermal-hydraulic phenomena were also observed, such as the 'simmer' phenomenon. If a volume between two isolation devices is filled with water, the water can heat up when the reactor starts up, and this can cause the deformation of parts, preventing their actuation: this can affect pipe sections between two separate valves, or valves with two gates such as the SIS valves outside the containment. Instances of failure-to-open on RHRS valves had been observed in the early 1980s. Measures were taken to prevent this type of problem, for example by installing an 'anti-simmer device' in the double gate valves in the SIS.

[756] Known as 'high-cycle fatigue', as opposed to 'low-cycle fatigue'.

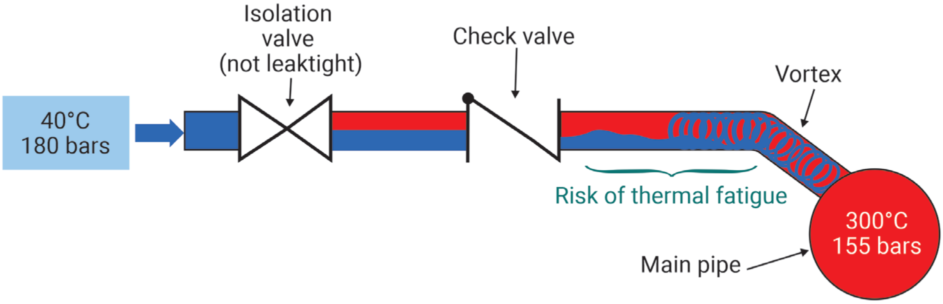


Figure 27.13. Simplified diagram illustrating 'Farley-Tihange' phenomena. Diagram taken from *La maintenance des centrales nucléaires* (Maintenance at Nuclear Power Plants) by Jean-Pierre Hutin – EDF/ Lavoisier Tec&Doc, 2016.

Only the 900 MWe reactors under the different programme contracts were affected, because of the architecture of their auxiliary systems; the reactors in other series had two isolation valves in series instead of a single valve.

In terms of the potential risk to safety, the leaks amounted to 'small breaks' (see Chapter 9); but these risks had to be analysed in more detail because complex hydromechanical phenomena were involved and because the leaks could be precursors to larger breaks.

The event affecting Unit 2 of the Dampierre-en-Burly nuclear power plant caused EDF to check the leaktightness of the valves and the condition of pipes at the elbows and welds on all the 900 MWe reactors, to prohibit their actuation between the start and end of each operating cycle, and to carry out pipe inspections if it was determined that the valves were not leaktight.

The event affecting Unit 1 of the Dampierre-en-Burly nuclear power plant was of particular significance: it was the first time a crack had been found not in an elbow or weld, but in a straight pipe section. Studies carried out by the operator showed that these cracks could penetrate the pipe wall in less than one cycle, i.e. before inspections could detect them. Once the problem was discovered, the operator carried out additional checks in straight pipe sections on 900 MWe reactors where leaking isolation valves had been found. The inspections detected a few cracks (Dampierre Unit 3, Fessenheim Unit 2, etc.); all the affected sections were replaced.

27.5.2. RHRS thermal fatigue at Unit 1 of the Civaux nuclear power plant

Thermal fatigue is a damage mechanism that EDF was faced with again in May 1998 when a leak (estimated at 30 m^3/h) appeared from a pipe in the residual heat removal system (RHRS) at Unit 1 of the Civaux nuclear power plant (N4 series) during a maintenance outage. This leak had been caused by cracks that looked like crazing, which had begun on the inside wall of the pipe and emerged on the outside wall at a pipe elbow (see Figure 27.14).

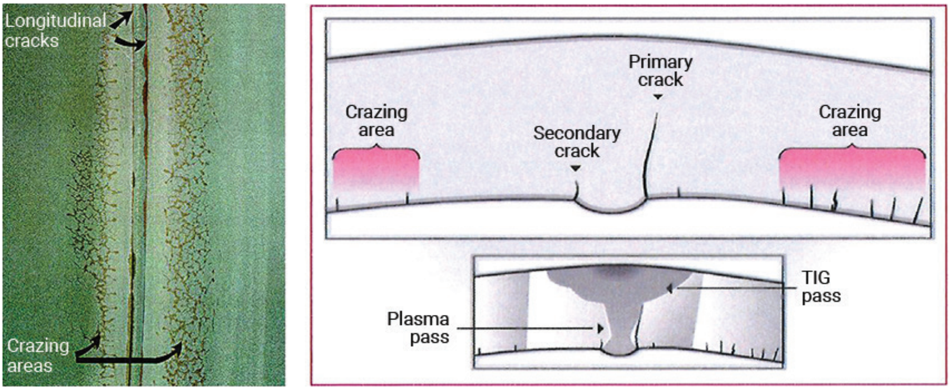


Figure 27.14. Inside of the pipe elbow where the leak at the Civaux NPP in 1998 originated. Crazing is visible on both sides of the weld bead. Image EDF (left) and IRSN – Source EDF (right).

The crazing area of the RHRS pipe (see Figure 27.15), made of austenitic stainless steel, was subject to significant temperature fluctuations downstream of a mixture of jets (one at 180°C, the other at 20°C) at a pressure of 27 bars. The cumulative operating time at large temperature differences (temperature differences of more than 80°C between the hot and cold fluids) had reached 1500 h.

The event in 1998 could not be predicted or explained by conventional mechanical fatigue analysis methods and criteria, such as those stipulated in RCC-M based on the assessment of a fatigue 'usage factor'[757].

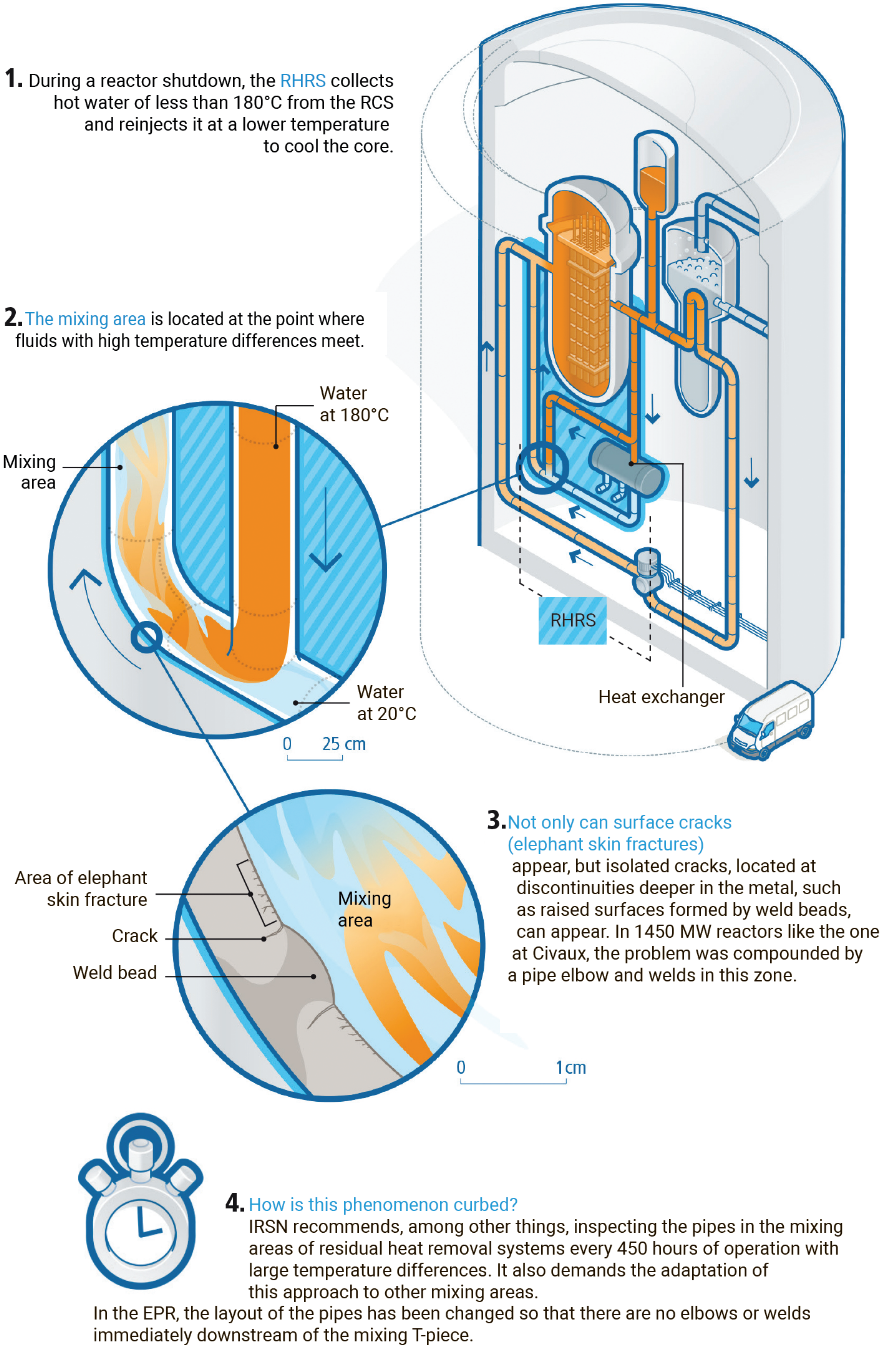
The event prompted EDF, in liaison with Framatome, to begin a new study in 1999 on 'thermal fatigue in mixing areas of systems important to safety' to find appropriate responses. A vast programme of actions in various domains was carried out, covering all the reactors in the nuclear power plant fleet:

- design review of the residual heat removal systems,
- determination of areas potentially vulnerable to thermal fatigue in reactors,
- non-destructive testing, assessments of cracked areas following removal,
- thermal-hydraulic simulations of flows and mixing of water jets at different temperatures in pipes, studies and research to understand the cause of the phenomenon.

IRSN, with support from CEA, also carried out a number of research and development projects on this subject[758].

[757] This usage factor is the ratio between the number of loads applied to a given component and the maximum number of loads indicated by the mechanical fatigue curve of the component's material.

[758] This work is discussed in more detail in Section 10.1.1 of the publication Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.



1. During a reactor shutdown, the RHRS collects hot water of less than 180°C from the RCS and reinjects it at a lower temperature to cool the core.

2. The mixing area is located at the point where fluids with high temperature differences meet.

3. Not only can surface cracks (elephant skin fractures) appear, but isolated cracks, located at discontinuities deeper in the metal, such as raised surfaces formed by weld beads, can appear. In 1450 MW reactors like the one at Civaux, the problem was compounded by a pipe elbow and welds in this zone.

4. How is this phenomenon curbed?
IRSN recommends, among other things, inspecting the pipes in the mixing areas of residual heat removal systems every 450 hours of operation with large temperature differences. It also demands the adaptation of this approach to other mixing areas.
In the EPR, the layout of the pipes has been changed so that there are no elbows or welds immediately downstream of the mixing T-piece.

Antoine Dagan/Spécifique/IRSN - Source : IRSN

Figure 27.15. Crazing in a pipe elbow of the RHRS at Civaux in 1998.

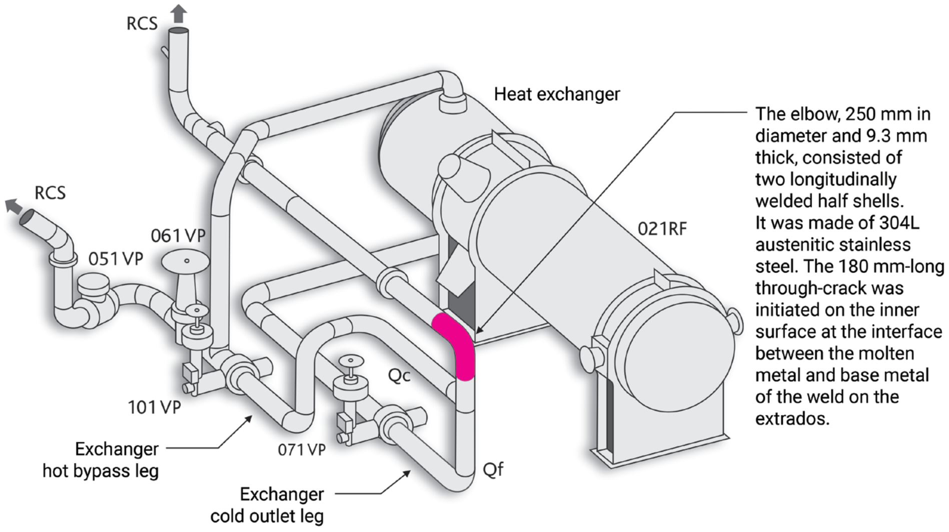

RCS
RCS
061 VP
051 VP
101 VP
Exchanger hot bypass leg
071 VP
Exchanger cold outlet leg
Qc
Qf
Heat exchanger
021RF
The elbow, 250 mm in diameter and 9.3 mm thick, consisted of two longitudinally welded half shells.
It was made of 304L austenitic stainless steel. The 180 mm-long through-crack was initiated on the inner surface at the interface between the molten metal and base metal of the weld on the extrados.

Figure 27.15 (continued). IRSN – Source EDF.

The ultrasonic inspections carried out from 1999 by EDF in the entire nuclear power reactor fleet showed that this was a generic problem: all the pipes examined had cracks, predominantly in areas where the surface condition was rough or at geometrical discontinuities such as weld roots. This prompted EDF to replace the mixing areas in RHRSs across the entire fleet, making improvements to reduce vulnerability to thermal fatigue: modification of the routing of the main line to reverse the direction of arrival of the fluids, elimination of longitudinal welds, limitation of the number of circular welds, moving them further away from mixing areas, grinding of welds, polishing of internal surfaces with a brush to improve the surface condition and eliminate any residual tensile stress.

Tests carried out by IRSN confirmed that, while the presence of a welded joint accelerates damage by thermal fatigue, this type of fatigue can also appear on uninterrupted sections of a material, as observed in the event at Dampierre Unit 1 in 1996. EDF thus extended inspections to areas without welds.

Based on the results of studies and research conducted on thermal fatigue, EDF defined a policy on operation, in-service monitoring and replacement for mixing areas, applicable to all reactors. Starting in 2000, ultrasonic inspections were carried out after every 450 h of operation on areas of residual heat removal systems subject to high temperature differences (following a recommendation made by IRSN) and the maximum operating time at high temperature differences was defined for all areas susceptible to this phenomenon.

Studies conducted on the takeoff area of the chemical and volume control system (CVCS) from the reactor coolant system – an area subject to much greater temperature differences than the RHRS elbows (up to 280°C) – suggested that the nature of the flow plays a more important role than the temperature difference, since the investigations showed that CVCS takeoffs in the fleet had little thermal fatigue damage. This finding has not been contradicted by in-service inspections conducted since then. An analysis of thermal fatigue risk at the takeoff of the pressurizer surge line and a T-piece linking the RHRS and CVCS systems led to the conclusion that these parts were not very susceptible, or indeed were not vulnerable at all, to thermal fatigue; an in-service inspection of a few T-pieces was nevertheless carried out (at the request of safety organizations).

All the research and development work on thermal fatigue has led to the view that areas subject to significantly lower temperature differences than those considered previously (before the event at the Civaux nuclear power plant in 1998) could be vulnerable to thermal fatigue (though it occurs after a larger number of thermal cycles); areas where there is a temperature difference of 50°C or more are now considered to be susceptible. Work on this complex topic is continuing, particularly to improve prediction of crack initiation by taking into account environmental effects (such as the chemical quality of the water).

27.6. Civil works: containment structures

The containment structure of a pressurized water reactor consists of a large cylindrical structure[759] built on a thick basemat[760] and topped with a dome; internal structures support the nuclear steam supply system. Three types of design are used for the containment buildings of pressurized water reactors in France:

- the first type (900 MWe reactors) has single pre-stressed reinforced concrete walls with a metal liner on the inside face, attached to the concrete by means of metal bolts and coated with a decontaminable, corrosion-resistant paint; it is a static containment[761];
- the second type (1300 MWe and 1450 MWe reactors) has double walls, where the inner wall is made from pre-stressed concrete and the outer wall from reinforced concrete; ventilation and filtration of the containment annulus between the two walls provides dynamic containment, complementing the static containment provided by the inner wall. It will be seen further on that liners made from composite materials (reinforced resins) have been installed against the intrados of the inner walls to improve their integrity;
- the third type (EPR) is a combination of the previous two: integrity is achieved by a metal liner on the intrados of the inner wall, supplemented by the dynamic containment associated with double-wall containments.

[759] The internal diameter is between 37 and 47 m, the internal height is between 55 and 67 m. The thickness of the wall (single or inner wall) is about one metre (more for the EPR).

[760] Several metres thick.

[761] Though it is combined with ventilation in normal operation.

The wall that ensures confinement of any radioactive substances released inside the reactor building is designed and sized to withstand accidents that can affect the nuclear steam supply system, which are:

- a break or rupture of a reactor coolant system pipe, in a loss-of-coolant accident (LOCA),
- a steam-line break (SLB).

The release of primary coolant or secondary system fluid, which may be contaminated, leads to a pressure (and temperature[762]) increase inside the containment building in a few tens of seconds (LOCA) or a few hundreds of seconds (SLB) after the rupture. This pressure can reach about five times atmospheric pressure. In these accident situations, the wall must provide the integrity specified (in the construction authorization decree for the reactors):

- for the 900 MWe reactors and EPR, a maximum leak rate of 0.3% per day of the total mass of gas in the containment,
- for the 1300 MWe and 1450 MWe reactors, a maximum leak rate of 1.5% per day of the total mass of gas in the inner containment wall.

The reactor building of a pressurized water reactor must also be able to withstand a certain number of internal and external hazards, whether of natural or human origin; in the case of the 1300 MWe and 1450 MWe reactors, it is the external wall that provides resistance to external hazards.

In-service monitoring of containment structures is described in special basic preventive maintenance programmes. This monitoring function focuses mainly on mechanical changes to the structures, but also considers the progression of defects and cracking. Besides detecting abnormal behaviour, the information obtained is used as input data for assessing the ‘end-of-life’ condition of the structure.

The instrumentation system used during tests takes readings on a regular basis to monitor structure performance. These measurements are taken at a periodicity that can range from 15 days to three months, depending on the observed or assumed deformation kinetics. In addition, partial visual inspections are also carried out, particularly at coastal sites, between the ten-yearly outages.

27.6.1. Anticipated degradation phenomena

In brief, the anticipated degradation phenomena for containment buildings – which must be managed – are:

- a reduction in the pre-stressing of cables,
- degradation mechanisms related to exogenic pathologies (due to the external environment) or endogenic pathologies (related to the concrete itself),

[762] From 140°C to 170°C, depending on the reactor type.

– corrosion of the metal liners.

Concerning the first, injecting cement grout into the cable sheaths (which has been done at some units) protects them from corrosion. But loss of pre-stressing can also be linked to the behaviour of the concrete, particularly 'shrinkage' (which happens when the concrete is formed, due to the departure of water [desiccation] and cooling) and, in service, creep. These phenomena, which lead to gradual slackening of the cables, are taken into account in design studies to ensure the concrete of containment buildings is still under compression, including in the accident situations mentioned earlier and at the end of its lifetime.

As regards pathologies, concrete swelling due to the alkali-silica reaction or delayed ettringite formation – phenomena brought to EDF's attention by IRSN at the end of the 2000s – should be given particular mention.

Both of these potential degradation mechanisms affecting containment buildings depend on the materials used in their construction; both are under study in research and development work[763]. The different reactor containment buildings in the nuclear power plant fleet have been ranked by EDF according to their degree of sensitivity to these two mechanisms.

27.6.2. Devices for direct monitoring of containment building concrete walls

The instrumentation systems installed in containment buildings can measure:

– settlement of structures on their foundation soil, their verticality,

– their mechanical 'response' (in terms of deformation and displacement) during testing,

– their temperature and, for some containment structures, their humidity,

– the tension of certain pre-stressing cables with sheaths that have not been injected with cement grout[764],

– the delayed deformation and displacement of the concrete (due to shrinkage and creep), which provide indirect information about the actual pre-stressing in the cables.

Rebar corrosion as well as concrete cracking and swelling are also monitored visually.

Monitoring of containment structures relies mainly on the following sensors (see Figure 27.16):

[763] Some of this work is discussed in more detail in Section 10.2.4 of Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

[764] But have been filled with grease to protect the cables.

- thermometers embedded in the concrete (thermocouples or Pt100 sensors[765]); their redundancy and service life are such that corrective measures have not been considered necessary in case of failure;
- vibrating-wire extensometers (see Figure 27.16) embedded in the concrete (local deformation measurements); some form part of the Optimal Monitoring System and must be replaced by extensometers on the surface of the wall in the event of failure;
- plumb lines (overall measurements of horizontal displacement);
- invar wires[766] (overall measurements of vertical displacement);
- spring scales on the few pre-stressing cables for which the sheath has not been filled with cement;
- levelling pots embedded in the basemat, which can be replaced where necessary by pots on the surface;
- altimetric reference marks;
- devices for measuring differential displacement.

By cross-checking these measurements, it is possible to assess and monitor overall displacements (settlement, verticality, variations in containment diameter or height), local deformations (in uninterrupted areas or areas with geometric discontinuities), and the tension of pre-stressing cables.

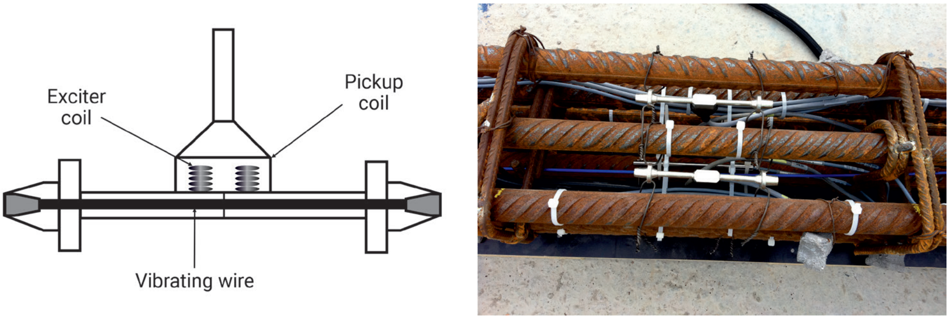


Figure 27.16. Left, diagram of a vibrating-wire extensometer. SFEN; right, view of two extensometers installed in a structural rebar grid before concrete is poured. EDF.

[765] A Pt100 sensor is a temperature sensor, also known as a resistance thermometer, made from platinum. The platinum element has a resistance of 100 ohms at 0°C. Compared to thermocouples, Pt100 sensors have the following advantages: a large temperature range, from -200°C to 850°C, an almost linear characteristic curve and high accuracy.

[766] The invar wire is an iron (64%) and nickel (36%) alloy. Its main property is that it has a very small expansion coefficient, which makes it ideal for use in high-precision measuring instruments.

27.6.3. Leak tests and measurements

Before a unit is commissioned, the containment (900 MWe reactors) or the inner wall of the containment (other reactors) undergoes overall leakage and strength testing by pressurizing the internal atmosphere with dry air at ambient temperature. The pressure applied is the design pressure, which is the accident pressure for 1300 MWe and 1450 MWe reactors; it is significantly higher than the accident pressure for containments with a metal liner, to represent the action of the liner in a LOCA because its expansion is opposed by the concrete, which stays cold (design pressure increased by 15% for 900 MWe reactor containments and increased by 10% for the Flamanville 3 EPR containment).

This test is then repeated during the reactor's operating life, at the time of the ten-yearly outages.

Unlike the maximum permissible leak rates specified for accident conditions, indicated above, the permissible leak rates under test conditions are obtained using a transposition factor defined by taking into account the difference between the test temperatures and pressures and those in accident conditions.

Prior to the tests, various visual inspections are carried out (on the accessible faces of the walls, liners, etc.) and leakage is measured at penetrations (equipment hatch, personnel airlock, fuel transfer tube between the reactor building and the fuel building, etc.). These measurements are also taken during each refuelling outage.

The (total) leak rate is measured by measuring the pressure, temperature and humidity of the air in the containment at the different pressure levels up to the test pressure.

French reactors also have a system known as SEXTEN, which provides continuous automatic monitoring of overall containment integrity; it is based on monitoring both pressure in the containment and air added for control purposes. In the event of significant leakage, it serves to determine which penetration is defective, as operators isolate each penetration one by one.

In the case of 1300 MWe and 1450 MWe reactors, the leak rate through the outer wall is also measured during ten-yearly outages. The most important goal is to prevent any leakage from the containment annulus to the outside environment other than through the annulus ventilation system. Consequently, negative pressure must be maintained throughout the containment annulus to compensate for suction phenomena due to the wind. Permissible leak rates have thus been specified for the external containment. The leak rate through the outer wall is also checked during each operating cycle (while the reactor is in operation) by performing periodic checks on the annulus ventilation system.

27.6.4. Main anomalies

A few anomalies have been detected by the in-service monitoring systems described above. The most significant concerns the inner containment wall on 1300 MWe and

1450 MWe units. During testing with air, some of them displayed a leak rate that exceeded the maximum admissible value, particularly at Unit 1 of the Belleville-sur-Loire nuclear power plant and Unit 1 at Flamanville. Satisfactory containment was still guaranteed by the annulus ventilation system.

Investigation campaigns and further tests were carried out to map the leaks. Areas of major leaks were found in particular areas, for example around the equipment hatch, but there were also more general leaks. Various mechanisms were put forward to explain the leaks:

- inadequacy of the resin injections between the different 'concreting lifts' due to shrinkage and creep mechanisms,
- drying of the concrete over time, gradual coalescence of original microcracks.

Finding the leaks and taking action to restore containment integrity required long outages at the affected reactors. Work consisted of first, injecting resin into the networks provided for this purpose, and second, installing a composite liner inside the containments, in the areas showing the most leakage. However, the effectiveness of these measures is not guaranteed in the long term, due to structural ageing, especially with the prospect of extending reactor operating lifetime beyond 40 years. EDF is exploring various avenues to address this issue.

Chapter 28
Fuel Management, Monitoring and Developments

The core of a pressurized water reactor consists of fuel rods[767] organized to form fuel assemblies. A fuel rod is a sealed metal tube made of zirconium alloy, known as cladding, which has very thin walls (approximately half a millimetre). The cladding contains the actual fuel (fissile material in pellet form). The main characteristics of fuel assemblies are described in Section 5.5, but as a reminder, these assemblies comprise 264 fuel rods (265 for the EPR), 24 guide tubes that serve for control rod insertion (for assemblies with control rods in 'clusters') and an instrumentation tube in the centre (except for the EPR). The guide tubes, grids and top and bottom nozzles form a skeleton that ensures assembly rigidity. Figures 28.1 and 28.2 show the various components that make up a fuel assembly.

As was seen in Section 5.2, when uranium and plutonium nuclei undergo fission, they emit neutrons which, in turn, are capable of bringing about further fission, thereby initiating the nuclear chain reaction. These fission reactions release a large amount of energy that is converted into heat. The reactor coolant, which enters the lower part of the core at a temperature of approximately 285°C, heats up as it rises up along the fuel rods and emerges from the upper part of the core at a temperature of approximately 320°C.

As explained in Chapter 5, the chain reaction is kept under control by two elements: neutron-absorbing components (also in the form of rods), which are present in control

[767] As a reminder, rod cluster control assemblies (RCCAs) are also made up of rods, but they serve to absorb neutrons.

RCCAs or shutdown RCCAs, inserted among the fuel assemblies to control reactor power and reactor shutdown; and boric acid in the reactor coolant, at concentrations that are adjusted to meet control requirements.

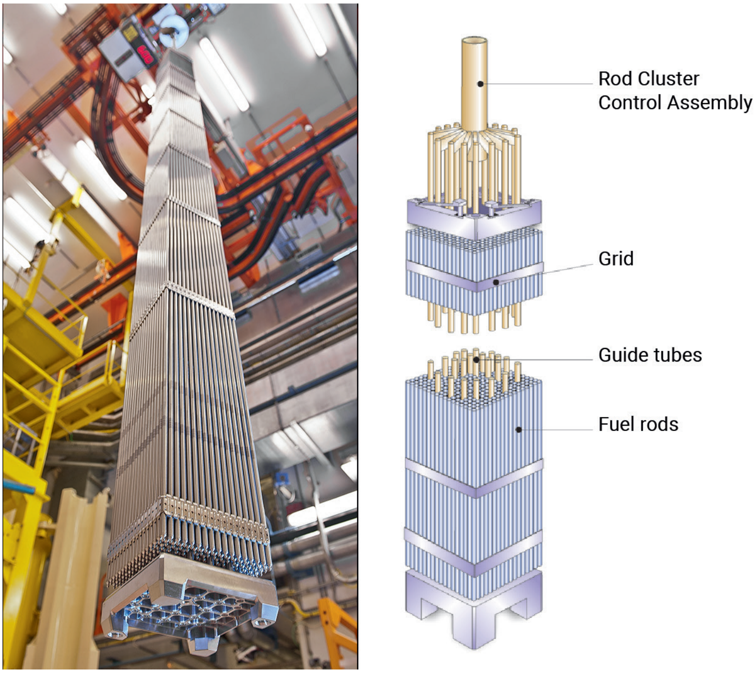
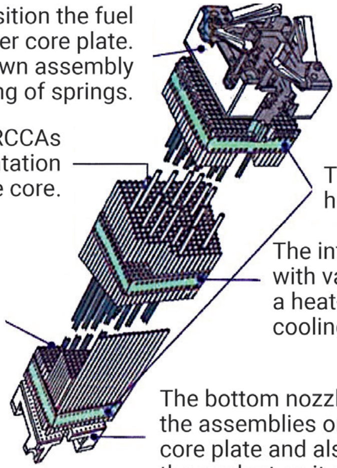


Figure 28.1. On the left, general view of a fuel assembly designed by Framatome. Éric Larrayadieu/Orano; on the right, diagram showing some of its components. Georges Goué/IRSN.



The top nozzle is used to position the fuel assemblies below the upper core plate. It also comprises a hold-down assembly consisting of springs.

The guide tubes guide the RCCAs and mobile internal instrumentation when they are inserted in the core.

The upper and lower end grids hold the rods in place.

The intermediate grids are fitted with vanes used to produce a heat-transfer effect to improve cooling of the fuel rods.

The fuel rods, in which energy-generating fission reactions take place.

The bottom nozzle is used to position the assemblies on the lower core plate and also distributes the coolant as it enters the core.

Figure 28.2. Description and function of fuel assembly components. IRSN.

Two types of fuel assembly are used in the reactors of the French nuclear power plant fleet:

- assemblies comprising fuel rods that contain uranium oxide (UO_2) pellets, which at present have a maximum uranium-235 enrichment of 4.2%[768]. These assemblies are manufactured in various facilities, both in France and other countries[769];

- assemblies comprising fuel rods that contain pellets composed of a mixture of depleted uranium oxide and plutonium oxide ($UPuO_2$) known as MOX fuel (see Section 5.7). MOX fuel is produced by the Orano Cycle MELOX facility located at Marcoule (Gard, France). The plutonium content[770] is currently limited to 9.08% (average per assembly), providing energy that is equivalent to the enriched uranium-based assemblies installed in the reactors[771].

To boost reactor availability and performance, Électricité de France (EDF) works with the relevant designers and manufacturers to study and improve fuel assemblies, as well as the associated procedures for use in reactors (i.e. the 'fuel management schemes'). Various fuel management schemes have thus been implemented by EDF since the first reactors in the French nuclear power plant fleet were commissioned, each scheme being characterized by:

- the type of fuel, its (initial) enrichment or content of fissile material and, where applicable, its initial neutron poison (gadolinium) content;

- the planned maximum burnup (average per assembly), also commonly known as the maximum burnup rate[772], for fuel removed from the reactor, which characterizes the quantity of energy extracted per tonne of (fissile: U or Pu) material, expressed in GWd/t;

- the nominal duration of an operating cycle;

[768] Situation in 2019, knowing that a limit value of 5% has been authorized.

[769] At present, there are only two remaining fuel assembly suppliers: Framatome ('AFA' assemblies) and Westinghouse ('RFA' assemblies). With regard to the Framatome assemblies, it is Framatome who manufactures the zirconium tubes (cladding) and performs final assembly (the fuel pellets are manufactured by Orano). The manufacturing plants are: FBFC at Romans-sur-Isère (France) and Dessel (Belgium) and ANF Siemens at Lingen (Germany). The Westinghouse assemblies are manufactured in Westinghouse plants at Västerås in Sweden, at Springfields in the United Kingdom and at the Juzbado (Salamanca) plant of the Spanish company ENUSA. EDF is supplied with Westinghouse assemblies under the terms of the European Fuel Group Agreement between Westinghouse and ENUSA.

[770] Plutonium content by mass, containing the fissile isotopes 239 and 241.

[771] The value was initially 8.65% (MOX fuel was first introduced in Unit B1 of the Saint-Laurent-des-Eaux nuclear power plant in 1997). Since 2017, the content has gradually been increased to 9.08% (up to an authorized value of 9.54%) in order to offset the degradation in the plutonium isotope vector obtained from reprocessing spent fuel and to maintain energy equivalence with 3.7% enriched UO_2 fuel.

[772] Or even 'maximum average discharge burnup per assembly'.

– the number of new fuel assemblies loaded into the core for each cycle during a reactor refuelling shutdown (generally one third or one quarter of the total number of fuel assemblies, this amount constituting a 'reload'[773]);

– the reactor operating mode (the possible modes being load-following[774], extended low-power operation, and extension or reduction of operation relative to the duration of the 'natural' cycle[775]); the operating mode determines the stresses to which the fuel is exposed, which must be taken into account in the associated safety demonstration documents.

The changes that have been made or are planned for the future involve increasing the admissible burnup rate (now possible thanks to research into high-performance rod cladding materials), extending operating cycle duration and using plutonium obtained by reprocessing spent fuel, while constantly maintaining an appropriate level of safety.

#FOCUS

Examples of fuel management schemes implemented in reactors of the French nuclear power plant fleet

The maximum burnup rate (average per assembly) was initially 33 GWd/t. Starting in the late 1980s, EDF introduced new fuel management schemes for its various reactor series, resulting in an increase in maximum fuel burnup. The maximum average burnup rate per assembly authorized in current fuel management schemes is 52 GWd/t, given that the average burnup rate of the assemblies discharged from the reactors is between 47 and 52 GWd/t, depending on the reactor series (situation in early 2019).

[773] For example, 40 new assemblies out of 157 are loaded for the 900 MWe series operating under the 'MOX Parity' scheme (see Focus feature below).

[774] Most operational nuclear power plants have been designed for flexible operation that can vary operating power to adapt to variations in consumer power demand; this means that the power plant 'follows' the load, i.e. the power draw arising from demand. Such adaptation is achieved in two ways. The first 'basic' method allows 'primary control' of the electric current frequency by up to ±2-3% in terms of power (an increase in demand results in a drop in frequency) and is carried out at the initiative of the facility operator, who adjusts the speed of the turbine generator. The second method (secondary control) involves electric current frequency control over longer periods of time (ranging from a few seconds to a few minutes). This is carried out at the initiative of the grid operator, who sends a digital signal to the power plant (via remote control) to modify its power level within a limit of an additional ±5%, with the possibility of varying this power level at a rate of 5% per minute between 30 and 100%. In the second control mode, 'grey' control rods, which are less absorbent than the 'black' control rods, are also deployed (see Section 5.6) to limit disruption of the neutron flux in the core as well as rod fatigue.

[775] Period of irradiation at the end of which the core is critical for a boron concentration of 10 ppm in the reactor coolant.

The implemented fuel management schemes are:

- for the 900 MWe reactors of the CPY programme contracts (except for those covered by the MOX Parity scheme), the GARANCE scheme (advanced PWR fuel management scheme designed for future cores), characterized by the use of assemblies based on UO_2 enriched to 3.7% uranium-235, with a one-quarter core reload. This scheme was implemented from 1987 onwards with a maximum authorized burnup rate per assembly of 47 GWd/t; it is still implemented in units that do not use MOX fuel ('non-MOX' units), but with a maximum authorized burnup rate per assembly of 52 GWd/t;

- for the 1300 MWe reactors, the GEMMES scheme (for safe development and modification of operating modes), characterized by the use of assemblies based on UO_2 enriched to 4% uranium-235, with a one-third core reload. Since fuel assemblies are used for a longer period under the GEMMES scheme, in order to ensure sufficient negative reactivity margins in the core at the beginning of the cycle while simultaneously limiting the boric acid concentration in the reactor coolant, a 'consumable' neutron poison, gadolinium oxide (Gd_2O_3), is incorporated into the fuel matrix. This scheme has been implemented since 1996;

- for the 900 MWe reactors of the first CP0 group (Fessenheim and Bugey reactors), the CYCLADES scheme (fuel cycle for increasing availability per safety assessment), characterized by the use of assemblies based on UO_2 enriched to 4.2% uranium-235, with a one-third core reload. Gadolinium oxide is used. This scheme has been implemented since 2000;

- for the 900 MWe reactors of the CPY programme contracts, the 'MOX Parity' scheme[776], characterized by the use of assemblies based on UO_2 enriched to 3.7% uranium-235 and MOX assemblies with an average content of 8.65% plutonium, with a one-quarter core reload. The maximum burnup rate is 52 GWd/t, as for the UO_2 assemblies ('MOX Parity 52'). This scheme has been implemented since 2007; as stated above, a 9.08% plutonium content has been authorized since 2017 in order to take into account the changes in isotope composition of the plutonium obtained from processing spent fuel from PWRs;

- for the 1450 MWe reactors, the ALCADE scheme (extending campaigns to achieve sustainable operational improvements), characterized by the use of assemblies containing UO_2 enriched to 4% uranium-235, with a one-third core reload, using gadolinium oxide. This scheme has been implemented since 2007;

- finally, it is also of interest to note the 1300 MWe reactor scheme, GALICE (featuring a limited increase in fuel irradiation during operation), characterized by the use of assemblies based on UO_2 enriched to 4.5% uranium-235, with a one-third or one-quarter core reload. The maximum burnup rate targeted for this scheme was 62 GWd/t. This fuel management scheme was implemented

[776] A 'hybrid GARANCE' scheme preceded the 'MOX Parity' scheme.

in 2009 at Unit 2 of the Nogent-sur-Seine nuclear power plant and then abandoned in 2014 after abnormal control rod drop times were observed in 2012 and 2013 (see Section 28.3.4 below).

Of course, any developments affecting fuel assemblies (cladding material, structural components, scheme, etc.) must be documented by EDF and submitted for approval by the French Nuclear Safety Authority (ASN); for matters of a certain importance or having a widespread impact, IRSN and the Advisory Committee for Reactors are consulted.

The procedure to obtain an authorization for a new fuel management scheme is generally long because it requires, on the part of safety organizations, an in-depth assessment of the information submitted by EDF substantiating that the fuel performs correctly under all normal, incident and accident operating conditions considered in the deterministic safety analysis, and subsequently is compliant with the associated criteria, some of which change over time – see Section 8.4.7 in the chapter on operating conditions, Chapter 9 on loss-of-coolant accidents and Chapter 35, which discusses rod cluster control assembly ejection accidents.

Furthermore, the safety demonstration for a fuel 'reload' is substantiated not only by a General Reload Safety Assessment File which, on the basis of operating condition studies for a reactor series and a fuel management scheme, defines the programme of studies to be carried out for each fuel reload and the key parameters[777] to be checked, but also by a specific reload document, namely the Specific Reload Safety Assessment File. Physical tests are performed when the reactor is restarted[778] and the results are recorded in a physical test report that contributes to validation of the safety demonstration and verification of core compliance with the studies presented in the safety report.

The safety demonstration support documents associated with fuel assemblies are the result of multidisciplinary studies: apart from demonstrating that the fuel assemblies perform correctly individually (in terms of criteria involving thermal-mechanics, mechanics, neutron physics, thermal-hydraulics, etc.) under normal conditions (including load-following, extended low-power operation, etc.) as well as incident and accident conditions, certain specific aspects may also need to be addressed, for example, the effect of using fuel assemblies that have different designs in the core, mainly on core thermal-hydraulics (changes in the distribution of water flow rates between assemblies due to different hydraulic resistance characteristics), or the effect of the fuel assembly loading plan (determined according to burnup rates) on the fluence received by the vessel.

Proper fuel assembly behaviour is an essential element of nuclear reactor safety. While in France fuel pellets are not considered as a confinement barrier as defined

[777] Technical acceptance criteria or parameters for decoupling from criteria.

[778] Tests performed under the rules for physical tests on restart.

in Chapter 6, even if they are capable of retaining a proportion of the fission products under operating conditions that are not excessively severe, the fuel rod cladding constitutes the first confinement barrier. Maintaining the integrity (leaktightness) of this barrier is a design requirement whereby fuel rods must be capable of withstanding the loads they are exposed to during operation or under degraded conditions. These loads correspond to normal, Category 1 operating conditions (base load operation, power variations for load-following and startup or shutdown transients) and Category 2 operating conditions of the deterministic safety analysis. One of the main objectives of the thermal-mechanical study of fuel rods is to show that, under Category 2 operating conditions, achieving maximum linear power density does not lead to pellet melting, thereby ensuring the integrity of the first confinement barrier.

Some of the loads to which fuel rod cladding is exposed in normal operation are briefly outlined below. They must be taken into account in the design phase of both fuel rod cladding and fuel assemblies, and must also be addressed in the safety demonstration.

In operation, a large part of the loads applied to cladding results from local power variations due to normal operating transients (load-following, extended low-power operation, etc.). During these transients, inside the fuel rod, the different levels of thermal expansion of the fuel pellets and the cladding may lead to rod damage, in particular as the result of interaction between the fuel pellets and the cladding. Furthermore, while little fission gas is released from the pellets into the free volumes of the rod up to a burnup rate of approximately 30 GWd/t, gas release increases rapidly above this level, bringing about an increase in internal pressure in the rod.

Depending on the cladding material, elongation of the fuel rods during reactor operation may also go as far as to create mechanical interference with the top and bottom nozzles on the assemblies. The assembly itself (guide tubes and nozzles) may interfere with the upper core plate in the event of excessive elongation. These risks are taken into account in design studies by checking that clearance is sufficient to avoid such interference.

Other loads that could potentially damage the cladding must also be considered, such as those relating to rod hold-down conditions in the cells of the fuel assembly grids, which may deteriorate due to irradiation and which, under certain conditions, may result in rod vibration and, ultimately, a loss of cladding integrity (‘cladding failure’).

Proper behaviour of the assembly structures is also of significant importance in controlling reactivity, because any lateral deformation[779] may slow, or even prevent, correct dropping of the rod cluster control assemblies in their guide tubes.

[779] Fuel assemblies, which are about four metres high, may undergo lateral deformation under the effect of hydraulic and mechanical loads, irradiation and temperature. Unlike this lateral deformation of the assemblies, which affects every rod in the assembly, the term ‘bowing’ is used to describe the deformation that affects a rod between two grids of the assembly and involves bending of a portion of the rod in question. This phenomenon has been taken into account in the safety demonstration since the initial design stage of 900 MWe reactors.

In normal operation, cladding integrity is monitored by continuously measuring the (specific) radiological activity of the reactor coolant. Any increase in this activity beyond predefined thresholds indicates a loss of fuel rod integrity. In this case, the facility operator must, in accordance with the operational limits and conditions, implement enhanced monitoring or even initiate reactor fallback and carry out shutdown within the specified time frame, after which the assembly or assemblies containing the failed rods must be located.

The aim of this chapter is to briefly address three topics[780]:

- the procedures implemented to monitor fuel rod integrity and the developments that shaped these procedures,
- cladding material developments,
- a selection of anomalies and significant events involving fuel rods or assemblies and the measures taken by EDF to remedy them.

28.1. Procedures for monitoring fuel rod integrity

Monitoring fuel rod integrity, more specifically, cladding integrity, relies on indicators calculated on the basis of radioactivity in the reactor coolant, which are associated with limit values (known as ‘radiochemical specifications’). Inspections are also carried out directly on those fuel assemblies suspected of having rod cladding failures once they have been pulled from the core.

28.1.1. Radiochemical specifications for reactor coolant

It should first be emphasized that, in a pressurized water reactor, several objectives underlie radioactivity measurements taken on reactor coolant and the associated radiochemical specifications:

- monitoring to detect any failure of the first confinement barrier, especially any possible generic damage phenomena (such as fretting, which will be addressed in Section 28.3.2) and implementing corrective or curative action;
- on one hand, reducing liquid and gaseous radioactive releases from the reactor to the lowest reasonably possible levels in terms of quantity and the risk of danger and on the other hand, likewise, reducing radioactive waste arising from treatment of the reactor coolant and, more generally, of the equipment that has been in contact with reactor coolant;
- reducing radioactivity from the reactor coolant system to the lowest reasonably possible levels to limit the doses received by workers – especially those who

[780] An entire book could be devoted to all the issues relevant to fuel and fuel monitoring reviewed in detail. Only a few noteworthy aspects have been selected here.

are called on to work in the vicinity of the reactor coolant system[781] – and by members of the public in the event of a release of reactor coolant to the environment (for example in the event of a steam generator tube rupture).

The remainder of this chapter will essentially address the first objective, given that monitoring reactor coolant activity and compliance with the associated requirements has a positive impact on the other objectives, namely by reducing the radiological impact of accidental steam generator tube ruptures with regard to the public and the environment.

The presence of fission products in the reactor coolant indicates that there are fuel rods with failed cladding in the reactor core. This is because, in normal operation, the fission products formed in the fuel matrix remain captive within the rods: if they are capable of leaving this matrix[782], for instance in gaseous form (xenon, krypton), they are confined in the leaktight cladding and accumulate in the free volumes of the rod, including in the gap between the pellets and the cladding (referred to as the 'pellet-cladding gap'). Actually, a very low level of radioactivity due to fission products is observed in reactor coolant regardless of the circumstances because of the inevitable contamination of the rods by fuel residues during their fabrication. However, an appreciable increase in radioactivity in the reactor coolant clearly indicates that leakage due to a cladding failure on one or more rods has given way to release of the fission products present in the pellet-cladding gap.

While, from a safety standpoint, it is obviously appropriate to attempt to avoid any failure of the first confinement barrier, its highly 'composite' nature (there are, for example, more than 50,000 fuel rods in a 1300 MWe reactor core) and the need to take into account industrial constraints (refuelling can only be performed during a reactor shutdown) have led to a certain momentary tolerance of cladding failures, which has resulted in setting thresholds to limit the level of radioactivity in reactor coolant. This contamination is, of course, taken into account in studies on the radiological impact of operations conducted under normal, incident and accident operating conditions.

The major problem encountered when setting the thresholds arises from the difficulty of correctly evaluating the state of the first confinement barrier during an operating cycle. This is because there is no simple method for establishing the condition of the fuel rod cladding in terms of the number and size of defects based on readily available data (consisting primarily of the monitored radioactivity produced by a few of the main fission products). Since the radioactivity released due to a defect depends on several unknown parameters that are not directly apparent (size, location, local thermal-hydraulics, rod burnup and heat transfer, etc.) and given that knowledge on the

[781] For example, those carrying out radiographic inspections of the system components, even after they have been drained. Deposits of radioactive substances originating from the fuel (see Section 31.1) as well as radiation-activated structural corrosion products may remain on the surface of these items.

[782] Through various mechanisms, such as diffusion and recoil, the latter being due to high-energy neutron impact (elastic diffusion theory).

physical phenomena involved in the release of fission products is still less than perfect, the models for 'predicting' defects on the basis of the radioactivity in the reactor coolant involve significant levels of uncertainty and the number and size of defects can only be reliably determined after the event, once the reactor has been shut down and the assemblies unloaded.

Furthermore, beyond the direct release of the (mainly gaseous) fission products initially present in the free volumes of the rod, the consequences of a loss of integrity in the first confinement barrier may be much more significant.

For instance, in the event of a cladding failure, or 'primary' failure, reactor coolant may penetrate into the pellet-cladding gap and vaporize there, resulting in radiolysis phenomena, oxidation of the internal wall of the cladding and pellet oxidation, thereby producing hydrogen. Over time, a significant quantity of hydrogen may be absorbed by the cladding and lead to 'secondary' defects in the cladding. However, although the mechanisms are well identified, it is not currently possible to derive models capable of predicting the conditions of cladding failure[783] associated with these secondary defects.

In the event of a significant cladding failure, water can penetrate in liquid form into the pellet-cladding gap and erode the fuel, thereby resulting in dispersal of solid fuel particles in the reactor coolant system. In extreme cases, fuel may emerge in the form of pellet fragments, or even whole pellets. Only very little of the dispersed fuel remains in suspension in the reactor coolant, and instead is deposited on the surfaces of reactor coolant system components, especially in heat-exchange zones (such as fuel assemblies and steam generator tubes). While that proportion of the fuel which has been deposited on the fuel assemblies will be removed from the reactor coolant system during subsequent unit shutdowns, normal fuel replacement operations mean that the quantity of material dispersed outside the core will stabilize after a few cycles due to phenomena such as erosion, solubilization and redeposition and will persist until the reactor is dismantled. Such dispersal is therefore characterized by being virtually irreversible, to the extent that some of the dispersed fuel will remain present in the reactor coolant system and therefore outside the first confinement barrier for the reactor's entire operating lifetime. Furthermore, since part of the fuel material is exposed to neutron flux, fission occurs (therefore producing fission products), directly in the reactor coolant.

Finally, fuel dispersal results in alpha-emitter contamination of the reactor coolant. More specifically, the dispersed fuel has generally been exposed, at least during part of a cycle, to the neutron flux within the reactor core. As a result of neutron capture, alpha-emitting transuranic isotopes are formed in this fuel material in increasing amounts as burnup rises[784]. These radionuclides will then contaminate the reactor coolant system components and the fraction deposited in zones exposed to the neutron flux will undergo a rapid increase in activity from alpha-emitting isotopes. Thus, in addition to the gamma and beta radiation-emitting fission products, fuel

[783] The expression 'cladding failure' is commonly used to denote any loss of cladding integrity, whether due to a leaktightness defect, an actual mechanical rupture or another source of failure.

[784] It is important to note that, even without irradiation, uranium and plutonium are alpha-emitters.

dispersal results in the presence of alpha-emitters in the reactor coolant system which give rise to specific problems[785] in terms of worker radiation protection (risk of internal contamination[786]) and releases (concentrations of alpha-emitters in liquid and gaseous waste must remain below the detection limits set for each power plant according to a decision issued by ASN).

Since commissioning of the very first units in the French nuclear power plant fleet, EDF has therefore monitored indicators of radioactivity in the reactor coolant, with associated thresholds, instead of referring to parameters related to fuel condition, which are frequently extremely difficult to determine. However, beyond specifying thresholds and measures to be taken in the event of these thresholds being exceeded with the aim of limiting radioactivity in the fluid lines, maintaining cladding integrity must be regarded as an objective in itself, given the importance of the first confinement barrier, and this should encourage facility operators to consider beneficial changes to fuel assembly and fuel rod design.

Several indicators have been used to monitor reactor coolant activity since the first units of the French nuclear power plant fleet were commissioned, and the associated threshold values have likewise evolved over time. The meaning of these indicators is briefly described in the Focus feature below. The following is merely intended to provide a very brief overview of these changes[787].

For plant units 1 and 2 of the Fessenheim nuclear power plant, EDF proposed applying operational radiochemical specifications derived from those established by the constructor, Westinghouse (in their pre-1975 version), which were determined based on the 1% cladding failure rate selected for design of the radiological protection and waste treatment systems, together with acceptable orders of magnitude of the radiological impact at the site boundary, in particular in the event of a steam generator tube rupture accident, discussed in Section 8.1 of this book. The safety organizations, however, considered these radiochemical specifications to be inadequate, which led, from the commissioning of these two units in 1977, to the following reactor coolant radiochemical specifications:

- (A): the Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN) was to be notified when the specific activity of the reactor coolant exceeded 10 Ci/t (370 GBq/t) for 'total gases'[788] or 1.12 Ci/t (44 GBq/t) for the iodine-131 equivalent (see Focus feature below);

[785] Described in detail in the Focus feature in Section 1.1.1.

[786] Other radionuclides (such as cobalt and iodine) may contribute to contamination.

[787] For further information, readers may refer to other sources such as, for example, the ASN website https://www.asn.fr/Informer/Actualites/Centrales-nucleaires-EDF-Combustible, public editions of the safety reports for each reactor series, or alternatively the OECD/NEA document entitled Leaking Fuel Impacts and Practices, NEA/CSNI/R(2014)10 of 18 July 2014, which includes radiochemical specifications for reactor coolant adopted at that time in different countries (including France).

[788] Xenon and krypton isotopes.

it was considered that this would correspond to a cladding failure rate of approximately 0.03%;

- (B): reactor fallback was to be initiated to achieve a shutdown state as soon as a threshold of 300 Ci/t (11,100 GBq/t) for 'total gases' was reached. Furthermore, iodine-131 equivalent activity had to remain below 1 Ci/t (37 GBq/t) in normal operation; beyond this value, enhanced monitoring[789] and corrective measures had to be implemented (load-following operation was also suspended). Continuation of operation was tolerated for three months at an iodine-131 equivalent activity between 1 and 2 Ci/t. Continuation of operation at power at an activity between 2 and 3 Ci/t required the explicit consent of the Central Service for the Safety of Nuclear Installations; beyond 3 Ci/t, reactor fallback to a shutdown state had to be initiated within 6 h;
- (C): during power transients, exceeding the iodine-131 equivalent thresholds defined in (B) was accepted for a maximum period of 48 h, as long as a limit defined as a function of power was observed.

Following commissioning of the Fessenheim reactors, the radiochemical specifications for reactor coolant underwent successive changes, making them more stringent and introducing new indicators in response to specific problems encountered; without going into detail, some changes occurred in response to:

- the request submitted by EDF to be allowed, under certain conditions, to return non-leaktight assemblies to service (particularly from 1979 to 1980),
- baffle jetting phenomena (see Section 27.3.1 – 1981-1984).

Some of the thresholds adopted from 1997 onwards are stated in generic terms below:

- in relation to total gases:
  - 150 GBq/t for the enhanced monitoring threshold (and initiation of a power transient to measure the 'iodine peak',[790] – a measure which had been introduced back in 1987 at the request of the Central Service for the Safety of Nuclear Installations),
  - 500 GBq/t as the threshold for initiating reactor fallback to a shutdown state in less than 48 h,
  - 1000 GBq/t as the threshold for initiating fallback in less than 8 h;

[789] A sample of reactor coolant is regularly taken for gamma spectrometry analysis at a chemistry laboratory at the facility. In enhanced monitoring mode, this sampling operation is carried out several times per week.

[790] This involves reducing power to cause iodine isotopes to emerge from any small cladding defects that retain the isotopes when the reactor is operating stably, but could increase the radiological impact of transients such as a steam generator tube rupture.

- with regard to the iodine-131 equivalent: 4 GBq/t as the enhanced monitoring threshold, 20 GBq/t as the threshold for initiating reactor fallback to a shutdown state in less than 48 h, 40 GBq/t as the threshold for initiating fallback in less than 8 h;
- for the new indicator, iodine-134, used in relation to fuel dispersal risks, the thresholds[791] are 5 GBq/t for enhanced monitoring and 10 GBq/t is the threshold for initiating reactor fallback to a shutdown state in less than 48 h (1 GBq/t corresponds to the dispersal of 5 to 7 grams of UO_2 fuel).

In 2002, radiochemical specifications more stringent than those stated above were adopted for the entire nuclear power plant fleet following fuel assembly damage observed in 2000 at Unit 3 of the Cattenom nuclear power plant (1300 MWe reactor) which was attributed to fretting (see Section 28.3.2) and had affected 92 rods (mainly from the third cycle and, to a lesser extent, from the second cycle). The threshold for triggering enhanced monitoring based on the total gases indicator was set to 50 GBq/t and, if the threshold was exceeded, this would lead to enhanced monitoring of the specific alpha-emitter activity of the reactor coolant and measurement of the ratio of the specific activity of caesium isotopes 134 and 137 (or the 'caesium isotope ratio'[792], $^{134}Cs/^{137}Cs$), this ratio being associated with the threshold for initiating reactor fallback to a shutdown state in less than 48 h[793]. The thresholds for the iodine-131 equivalent adopted in 1997 were not modified. With regard to iodine-134, the threshold for triggering enhanced monitoring was lowered to 2 GBq/t, while the threshold for initiating fallback to reactor shutdown in less than 48 h remained at 10 GBq/t.

In the specific case of Cattenom Unit 3, more restrictive or additional thresholds had been applied to allow immediate continuation of facility operation, specifically:

- an increase of 5 GBq/t in the specific activity of xenon-133 was to trigger measurement of the $^{134}Cs/^{137}Cs$ ratio;
- reactor fallback to a shutdown state was to be initiated in less than eight days if the measured specific activity of iodine-134 reached 1 GBq/t, or if the specific activity of xenon-133 rose by 20 GBq/t with a caesium isotope ratio greater than 0.8.

[791] These threshold values actually involve the additional activity that comes from the calculated theoretical specific activity of 'residual' contamination.

[792] By measuring this ratio, it was assumed that this would make it possible to differentiate rod defects according to the operating cycle in which the rods had been loaded into the core (the value being below 0.8 for first-cycle rods).

[793] Later, in 2008, EDF stated in the *Document standard des spécifications radiochimiques du palier 1300 MWe* (Standard Document on Radiochemical Specifications for the 1300 MWe Series) that, given the difficulties involved in interpretation (especially when several non-leaktight assemblies from different irradiation cycles are present in the core), it did not wish to pursue application of the principle whereby the value of the caesium isotope ratio formally triggered the decision to initiate reactor shutdown within 48 h, which was accepted in 2012 by ASN.

In June 2002, the new generic radiochemical specifications proposed by EDF were accepted by the French safety authority, which furthermore requested[794] that "any fuel assembly that has been found to be non-leaktight during refuelling no longer be reloaded, without pulling the damaged rods or invalidating the measurement by appropriate inspection", a significant change with regard to refuelling practices in force since the 1980s.

However, following the introduction of the new generic radiochemical specifications, rod integrity failures, attributable to the same fretting phenomenon, were observed at Cattenom Unit 4 and Nogent Unit 2. This phenomenon was then classed as 'generic' for 1300 MWe reactors. Reinforced provisions were then adopted for all these reactors in 2003, including:

- for the total gases indicator, a threshold for enhanced monitoring and triggering measurement of the caesium isotope ratio lowered to 10 GBq/t, a threshold for initiating reactor fallback to shutdown in less than 48 h lowered to 50 GBq/t if the caesium isotope ratio is greater than 1.4 (a value allowing between 20 and 30 fretting-type defects on third-cycle rods), otherwise maintained at 500 GBq/t;
- for the indicator relating to the specific activity of iodine-134, a threshold of 1 GBq/t for enhanced monitoring and a threshold of 5 GBq/t for initiating reactor fallback to a shutdown state in less than 48 h.

In 2008, EDF, thinking it had remedied the risk of fuel rod fretting damage, wished to return to the radiochemical specifications common to all reactors in the nuclear power plant fleet. For their part, safety organizations were of the opinion[795] that the reinforced provisions relating to the thresholds associated with the total gases and iodine-134 indicators should be maintained for the 1300 MWe reactors.

The above demonstrates, if there was any need, how difficult it is to use a set of indicators to form a clear picture of the state of damage to cladding in the core of a pressurized water reactor.

In early 2019, the thresholds in force arising from the latest adjustments to the radiochemical specifications for the reactor coolant were as follows:

- for total gases:
    - for 900 MWe reactors (apart from Fessenheim and Bugey), 1300 MWe reactors and those at the Civaux nuclear power plant[796]: 10 GBq/t as the threshold for enhanced monitoring (and stopping load-following), 150 GBq/t for initiating reactor fallback to a shutdown state in less than 48 h[797], 1000 GBq/t for initiating fallback in less than 8 h;

[794] Letter DGSNR/SD2/703-2002 of 27 June 2002.

[795] This issue is addressed in the position paper entitled Safety and Radiation Protection at French Nuclear Power Plants in France in 2009 – IRSN's Position, DSR report 383.

[796] Developments are under way for the other reactors.

[797] Normal Shutdown/Steam Generator state.

- for the iodine-131 equivalent (on all reactors):
  - during operation at power: 4 GBq/t for the threshold for enhanced monitoring (and stopping load-following), 20 GBq/t for initiating reactor fallback to a shutdown state in less than 48 h, 40 GBq/t for initiating fallback in less than 8 h;
  - during power or shutdown transients: restart or continuation of operation at power are prohibited above 150 GBq/t;
- for xenon-133 and a new indicator, the ‘xenon isotope ratio’ (ratio of the specific activity of xenon isotopes 133 and 135 – see Focus feature below), for all reactors:
  - beyond a specific activity of xenon-133 of 185 MBq/t, the reactor is considered not to have any cladding failures if the xenon isotope ratio does not exceed 0.9;
  - it is assumed to have a failure if the ratio exceeds this value or if the specific activity of xenon-133 exceeds 1 GBq/t; these thresholds determine the fuel assembly inspection strategy at the end of the cycle (see Section 28.1.2);
- for iodine-134, on all reactors, thresholds are set for the transition to enhanced monitoring (and stopping load-following) as well as for initiating fallback to a shutdown state in less than 48 h as a function of iodine-134 activity at the beginning of cycle and as the cycle progresses (measured in terms of burnup) with the aim of revealing possible dispersal of fissile material during the current cycle.

These radiochemical specifications will of course continue to change in the future, for all or just some of the reactors in the nuclear power plant fleet, in line with the fuel strategies implemented by EDF, depending on any events that may occur (such as detection of new types of failure), or alternatively in order to respond to safety improvement objectives. In this respect, and following comments from the safety organizations, EDF intends to lower some thresholds in order to reduce the radiological impact on the public and the environment of any release that might arise from steam generator tube rupture (objective set in the context of the project to extend reactor operating lifetime beyond 40 years and in view of the fourth ten-yearly outage of 900 MWe reactors). This is explained in detail in Section 30.5.

#FOCUS

Radiochemical indicators for reactor coolant

Only some of the radiochemical indicators for the reactor coolant used by EDF have been mentioned above with the aim of making this complex issue easier to understand. This Focus lists all the indicators which are being or could have been used or indeed are being or have been discussed between EDF and safety organizations:

- **total gases**: measuring the specific activity of total gases (xenon and krypton isotopes) in the reactor coolant provides responsive monitoring of the condition of fuel assembly cladding because fission gases can generally escape quite easily through cladding defects; it is, however, very difficult to link this measurement to the number of defects, except in certain very specific cases in which the origin of the defects present in the core is known;

- **^{133}Xe, xenon isotope ratio**: ^{133}Xe and ^{135}Xe are taken into account in the total gases indicator. ^{133}Xe is one of the main fission products; its half-life is sufficiently short (5.2 days) for it to be at equilibrium after a few weeks of reactor operation and sufficiently long for its specific activity to be effectively measurable by sampling; finally, in the event of cladding failure, an increase in its specific activity in the reactor coolant is rapidly detected, even in the absence of any significant variation in the specific activity of iodine isotopes. After the Cattenom Unit 3 event, EDF also chose to monitor the ratio of the specific activities of xenon isotopes 133 and 135 (^{133}Xe/^{135}Xe) which, according to EDF, would make it possible to detect the occurrence of (small) defects as quickly as possible and implement specific reactor coolant monitoring (in particular alpha activity);

- **^{131}I equivalent**: iodine-131 is an important indicator due to its radiotoxicity and its half-life (approximately eight days); to obtain a radiation protection indicator associated with the risk of internal thyroid contamination, an iodine-131 equivalent activity was defined as the sum of the specific activities of the various iodine isotopes weighted by their dose coefficients;

- **activity at iodine peak**: the various iodine isotopes only escape from a failed fuel rod when the cladding defect(s) are large or during power transients resulting in water ingress into the cladding and 'leaching' in the pellet-cladding gap. A certain amount of iodine may thus be located in the reactor coolant – in addition to that measured in steady-state operation – during a reactor trip resulting from a steam generator tube rupture, leading to large releases. Accordingly, since 1987, to check that ^{131}I equivalent activity does not at any time exceed a value of 150 GBq/t, including during transients, a power transient (load reduction) is carried out when the specific activity of total gases reaches 150 GBq/t. Returning the reactor to power is prohibited if the iodine peak exceeds 150 GBq/t;

- **^{134}I**: with a short half-life (less than one hour) and trapped in the pellet-cladding gap, iodine-134 is hardly ever released through cladding defects unless they are very large. When significant amounts of iodine-134 are present in the reactor coolant, it is mainly produced by two mechanisms: first, nuclear fission of dispersed fuel deposited in the zones exposed to neutron flux and, second, major defects that bring the fuel into direct contact with the reactor coolant.

To date, iodine-134 is the best indicator of fuel dispersal in the reactor coolant on pressurized water reactors, even if the associated activity is only an imperfect representation of the amount of fuel that has left or may leave the rods;

- **caesium isotope ratio**: the ratio of the specific activities of caesium isotopes 134 and 137 ($^{134}Cs/^{137}Cs$) was included in the reactor coolant radiochemical specifications in order to evaluate the burnup of rods with cladding failures. Given the associated uncertainties, it must however be used with caution;
- **alpha activity**: due to the questions raised by the presence of alpha-emitters in terms of radiation protection, release and waste, it seemed appropriate to set a limit value for alpha activity as such, regardless of the amounts of corresponding materials dispersed in the reactor coolant system, which are difficult to evaluate.

28.1.2. Inspections and measurements carried out directly on fuel assemblies

Fuel assembly cladding integrity inspections are carried out during a reactor core refuelling shutdown when the activity of the reactor coolant at the end of the cycle does not comply with a certain number of criteria capable of indicating any traces of cladding failure[798], namely:

- specific activity of xenon-133 below 1 GBq/t,
- 'xenon isotope ratio' ($^{133}Xe/^{135}Xe$) below 0.9 (see Focus feature above),
- absence of 'iodine peak' during transient.

Several measures may be taken by EDF to directly inspect fuel assemblies that have been removed from the reactor:

- liquid penetrant testing in the refuelling machine mast,
- liquid penetrant testing in a dedicated fuel building cell ('FB cell'),
- inspections of the rods themselves

These measures are accompanied by other types of inspection, more geometrically oriented, carried out on the assembly structures, such as those performed using the portable fuel assembly measuring device known as DAMAC[799] (see Figure 28.3). The purpose of these inspections is not to check cladding integrity, but to provide a clearer

[798] Otherwise, the reactor is declared in presumption of fault; if other thresholds are exceeded, this suggests the presence of a 'cladding failure' or a 'serious cladding failure'.

[799] *Dispositif amovible de mesure des assemblages combustibles* (mobile unit for taking measurements on fuel assemblies).

picture of the behaviour of fuel assembly components, as any observed changes may lead to other problems, not necessarily cladding failures. Only assemblies unloaded from a few reactors considered to be the most sensitive are inspected in this manner.

DAMAC, developed for use in the spent fuel pool building, is designed to measure lateral deformation of fuel assemblies by carrying out ultrasonic measurements of the lateral offset exhibited by each fuel rod spacer grid relative to the centre axis of the assembly. This examination serves to avoid refuelling or 'clustering' the reactors in question using fuel assemblies that have deformations capable of preventing the rod cluster control assemblies from dropping correctly.

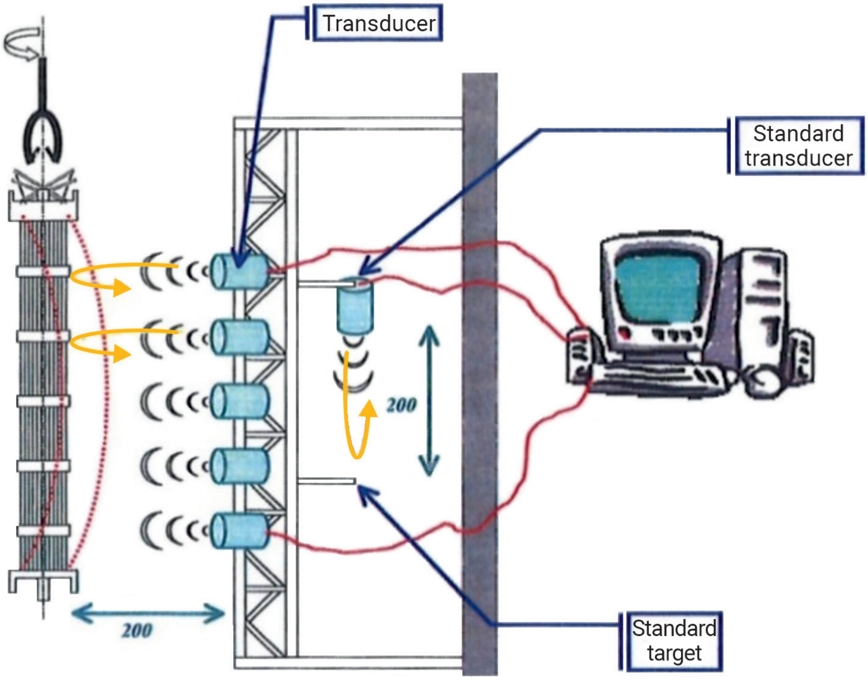


Figure 28.3. DAMAC measuring device (source EDF).

28.1.2.1. Liquid penetrant testing in the refuelling machine mast

On reactor shutdown, once it is presumed that there is a failure[800], the facility operator inspects every assembly unloaded from the reactor core using liquid penetrant test equipment installed in the mast[801] of the refuelling machine, developed in the 1980s. In order to be effective, this inspection must be carried out within 20 days

[800] Measurements are not systematically taken on the refuelling machine.

[801] The mast is a metal structure (skirt) with a three-sided section, reinforced circumferentially at different levels, and is suspended from the handling gantry. Fuel assemblies are lowered (loading) or raised (unloading) in this structure. Various items of equipment are installed inside the mast.

(four half-lives of xenon-133, the isotope measured using this equipment) following reactor shutdown. This period is sufficient for unloading the fuel assemblies if there are no particular problems.

The measurement principle is as follows: when raising a fuel assembly from its location in the reactor core to the mast of the refuelling machine, the difference in pressure inside and outside each fuel rod differs by approximately 0.9 bar (vertical displacement of approximately nine metres); this causes fission products (including xenon-133) to be released from any failed rods into the water present in the refuelling machine and into the water in the reactor pool. Once in the top position in the mast, the assembly under inspection is swept with air which carries away the fission products emitted by any failed rods. The mixture of air and fission products is drawn into an activity counter where the activity concentration of xenon-133 is measured continuously.

Fuel assemblies can be divided into three categories based on analysis of the results:

- healthy assemblies,
- questionable assemblies,
- failed assemblies.

Healthy assemblies that are not reloaded are dispatched to the reprocessing plant after spending a period of time in the spent fuel pool. Failed assemblies are packaged in 'bottles'[802]. As for the questionable assemblies, they are inspected in the fuel building (FB) cell.

28.1.2.2. Liquid penetrant testing in the FB cell

Fuel assemblies are inspected in the FB cell when:

- the fuel assembly cooling time is greater than 20 days (liquid penetrant testing in the refuelling machine is then inappropriate), or
- the fuel assemblies are declared 'questionable' after liquid penetrant testing in the refuelling machine to establish whether they are leaktight before they are reloaded into the reactor, or
- liquid penetrant testing has not revealed the failed assembly/assemblies even though a 'presumed failure' has been detected; all the fuel assemblies to be reloaded must then undergo liquid penetrant testing in the FB cell.

The fuel assembly to be inspected is then placed in the FB cell, a leaktight, thermally insulated space located in the spent fuel pool. The cell is equipped with water lines for heating and cooling the water in the assembly and an air system for air-sweeping the assembly. Heating the water encourages the release of radionuclides into the cell if

[802] Depending on the level of burnup reached by the failed fuel assembly, EDF may decide to search for the non-leaktight rod(s) and, after replacing it (them), to reload the assembly into the reactor to continue irradiation.

cladding failures are present. Radioactivity is measured by in-line counting on a sample taken from the water lines or from the air sweeping system.

Unlike the liquid penetrant testing in the refuelling machine, where measuring is conducted continuously, in the FB cell, fission product activity is measured after a certain time delay, which allows radionuclides to accumulate, making the method more sensitive. FB cells are, however, more sensitive to contamination phenomena, in particular by corrosion products deposited on the assemblies, which may complicate measuring caesium isotope activity.

Following inspections in the FB cell, the fuel assemblies are divided into two categories:

- healthy assemblies,
- failed assemblies.

If, after the measurements taken in the FB cell, an assembly is considered non-leaktight, it is not reloaded into the reactor, in accordance with ASN's the French safety authority's request made in 2002 (see above).

It should be noted that, until 2002, the size of the defects was characterized on the basis of the fission product release kinetics in order to identify fuel assemblies that could be reloaded. This practice has since been abandoned.

28.1.2.3. Inspections performed on fuel rods

▶ Ultrasonic examination

The various existing devices for locating failed fuel rods in a fuel assembly, such as the tools developed by Areva (ECHO 330 and single probe ECHO) or by Westinghouse (AFIS), are based on the same principle, i.e. measuring the attenuation of an ultrasound signal as it travels over part of the circumference of the cladding, where attenuation reveals the presence of water in the pellet-cladding gap at the measuring point. Ultrasonic sensors are arranged on a 'comb' inserted into the spaces between rods. All rods are inspected on all four sides of the fuel assembly under examination. The device is placed on the racks of the spent fuel pool and the assembly to be examined is suspended from the bridge crane. Each probe is calibrated using a mock-up containing standard rods, some filled with dry sand simulating leaktight rods and some filled with a mixture of sand and water simulating the failed rods. The facility operator uses the results to establish a signal attenuation threshold 'S', corresponding to a failed rod (percentage of signal attenuation in the case of a rod filled with water) for each probe.

Measurements are taken at the bottom of the fuel rods, immediately above the first grid, a zone where cladding may potentially have suffered damage (due to fretting, loose parts or other reasons) and water may therefore be present inside the rods. The signal attenuation values observed for the various rods are compared with the probe threshold 'S' and the rods are divided into three categories: leaktight, failed (non-leaktight) and questionable. In the latter case, a higher-level inspection may be carried out.

It is important to note that in this regard, if a fuel rod is not leaktight and there is no water at the point of inspection, there is a risk of reloading potentially non-leaktight assemblies in the reactor core. Furthermore, a certain number of factors may interfere with signal readings (such as deposits, pellet-cladding interaction, an oxide layer or others) which in this case entails a risk of overestimating the number of failed fuel rods.

The above-mentioned devices are used to locate failed rods in the fuel assemblies identified as non-leaktight during liquid penetrant testing in the refuelling machine mast or in the FB cell and that are intended to be reloaded (after replacing the defective rods, possibly by dummy rods).

▶ Other inspection techniques

A fuel assembly may undergo a closed-circuit TV inspection by scanning all four sides of the assembly using a video camera in the spent fuel pool, which may provide an initial view of a failed assembly. While the condition of the assembly's peripheral fuel rods is quite clear, it is frequently difficult to assess the condition of the rods located in the centre of the assembly. Slightly rotating the assembly can, however, provide valuable information (presence of loose parts, blistering, etc.) by offering a view between the rows of fuel rods. This examination may in some cases make it possible to identify one or more defective fuel rods and sometimes to directly establish the cause of failure. A recording of a TV inspection is always sent to the supplier of the failed fuel assembly in question for analysis purposes and to assess whether it is worthwhile or necessary to pull the rods.

For fuel assemblies supplied by Framatome, rods can be pulled using the 'fuel assembly repair station' (FARS). After disassembling the top end of the assembly, the upper plug of the fuel rod to be pulled can be gripped using a clamp. Once the assembly has been installed in a device called the 'fuel elevator', the rod is pulled by moving the fuel elevator downwards. A device records the pulling force, which must be below a specified threshold. For fuel assemblies supplied by Westinghouse, rods are pulled using the New Fuel Elevator Platform (NFEP) which operates along the same principle as the fuel assembly repair station.

Once pulled, an individual fuel rod can be examined in the fuel assembly repair station in order to locate any defects. This search is carried out by passing the pulled rod vertically through an eddy current coil to quickly explore the entire length of the rod and select which zones are to be examined using closed-circuit TV; a video camera equipped with special lighting is then placed sufficiently close to the rod to allow it to be examined under high magnification. A video recording is made as the rod travels. If a fault is detected, a freeze frame generally provides a more detailed view for examination. This type of televisual examination nevertheless remains complex.

Expert assessments may then be carried out on certain defective fuel rods in an appropriate laboratory.

The reliability of the fuel assembly and fuel rod inspection methods and devices presented above is actually quite relative, despite improvements made in the course of time (in particular beginning in 2007, when the instrumentation and control racks of the liquid penetrant test equipment of the refuelling machine were upgraded). More detailed analyses of the liquid penetrant test sequences have also been performed by EDF to identify any abnormal peaks in the recordings. As a result, liquid penetrant testing in the refuelling machine mast and in the FB cell may yield strange results that cannot be straightforwardly interpreted for decision-making purposes; consequently, it may happen that some questionable or even failed fuel assemblies are reloaded into reactors.

28.2. Operating experience feedback and changes in cladding material

The fuel rod cladding used in reactors of the French nuclear power plant fleet were initially made from Zircaloy-4 (except for those at Chooz A which were made of steel), a zirconium-based metal alloy containing tin and other elements. Zirconium was established as a cladding material for light water nuclear reactors mainly due to its low absorption of neutrons[803].

After some fifteen years of using Zircaloy-4 for fuel rod cladding, the reliability of the corresponding assemblies appeared to be relatively satisfactory up to burnup rates of approximately 45 GWd/t, with initial operating experience feedback from load-following behaviour reporting a cladding leak rate of the order of a few 10^{-5} due to hazards or mechanisms specific to the rods (manufacturing defects, etc.), independently of possible external causes of deterioration (such as baffle jetting and loose parts), and excluding accident situations.

However, from the 1980s onwards, with the increase in maximum burnup rates authorized for the various types of fuel in the nuclear power plant fleet, it was then found that Zircaloy-4 cladding underwent significant external oxidation in the reactor, leading to the formation of an outer layer of zirconium oxide, the absorption of hydrogen with the formation of zirconium hydride, possible spalling of the oxide layer which had formed and the formation of hydride blisters[804]. Consequently, fuel

[803] This is because it has a small thermal neutron capture cross-section.

[804] When in contact with cladding, water oxidizes the cladding in a reaction leading to the formation of a surface layer of zirconia and the absorption of some of the hydrogen released in the form of hydrides: these phenomena are commonly described by the term 'corrosion'. When the thickness of the layer of zirconia exceeds approximately 80 mm, it may spall, giving rise to particularly radioactive debris that may accumulate in the reactor coolant system and create 'hot spots'. Zones of cladding showing a significant presence of hydrides (known as hydride blisters or lenses) are fragile and contribute to crack formation, which could lead to cladding failure during incident or accident transients. Oxidation kinetics depend on the cladding temperature, which is approximately 350°C in normal operation, but may reach 450°C to 480°C under Category 2 operating conditions and even much higher values (above 900°C) under category 3 and 4 operating conditions, thereby entailing rapid oxidation. These different operating regimes (normal, incident and accident) are associated with technical acceptance criteria for the purposes of deterministic safety analysis (see Section 8.4.7).

assembly designers and manufacturers suggested using new zirconium-based alloys comprising niobium, which exhibit improved properties in terms of in-reactor oxidation and hydriding phenomena. In France, new fuel assemblies comprising fuel rods with cladding made from Zircaloy-4 have not been loaded into reactors since late 2016 and cladding of this type should no longer be used in reactors by 2022.

The phenomena described above raise a certain number of questions as to the resistance of cladding under accident operating conditions, such as ejection of a rod cluster control assembly, which is why in 2014 ASN requested that EDF implement compensatory operational measures until Zircaloy-4 cladding has been completely eliminated from reactors[805].

The development of new zirconium-based alloys for fuel rod cladding began in the 1980s. Fuel assemblies featuring cladding (or even other structural components) fabricated using these new materials have been authorized and loaded into reactors in successive stages, starting with a few 'forerunner' assemblies[806]. These new fuel products are being implemented based on French and international operating experience, the results of in-reactor monitoring programmes – monitoring changes in the dimensional characteristics of fuel assemblies and fuel rods (elongation [or growth], gaps between rods and rod bowing, oxide layer thickness on the cladding, etc.) as a function of burnup – and based on laboratory testing to establish the mechanical characteristics of the cladding materials under incident and accident operating conditions (with a particular focus on pellet-cladding interaction, loss of reactor coolant and ejection of a rod cluster control assembly).

It follows that from the late 1980s onwards, EDF fuelled its reactors using fuel assemblies supplied by Framatome in which rod cladding was manufactured using an alloy known as Massif 5 (M5®) in the 'recrystallized' state[807], containing niobium and other additives. Apart from better corrosion resistance, the M5® alloy also differs from Zircaloy-4 (which, for cladding, is stress-relieved[808]) by exhibiting less dimensional elongation in reactors[809]. More specifically, an early version of the M5® alloy was first used in French reactors in 1988 when a few fuel rods were loaded in the context of the 'X1 first phase' development programme. The introduction of fuel rods featuring M5® cladding then continued between 1990 and 1996 in the context of four experimental 'prequalification' programmes conducted to test different alloy grades.

M5® alloy cladding was not qualified until 1999, when Unit 2 of the Nogent-sur-Seine nuclear power plant was the first to be completely refuelled using assemblies containing fuel rods clad with this alloy. However, the structural components of these

[805] In this context, only those rods with cladding having an oxide layer thickness below 108 μm are kept in the reactor.

[806] Generally four in number.

[807] Material with a microstructure obtained using a recrystallization heat treatment to enlarge the grain size (equiaxial grains).

[808] In other words, which has undergone thermal stress relief to reduce internal stresses.

[809] At maximum authorized burnup rates, rod elongation observed after use in reactors amounts to a few centimetres for Zircaloy-4 and a few millimetres for M5®.

fuel assemblies (guide tubes, spacer grid straps, etc.) were still made of Zircaloy-4 (in the recrystallized state). It was not until 2004 that the first 'all M5' fuel assembly loads were loaded in Unit 2 of the Nogent-sur-Seine nuclear power plant. Refuelling with 'all M5' assemblies was then implemented under the ALCADE fuel management scheme for 1450 MW reactors in 2007 and for 1300 MWe reactors in 2015. The 900 MWe reactors are fuelled with UO_2 fuel assemblies supplied by Westinghouse or Framatome, together with MOX fuel assemblies supplied by Framatome, the Framatome design assemblies comprising M5® alloy cladding and Zircaloy-4 alloy structural components.

Between 2001 and 2008, around thirty fuel rods with M5® alloy cladding showed cladding failures during irradiation in the reactor. As soon as cladding failures were observed on rods with the M5® alloy cladding at Unit 2 of the Nogent-sur-Seine facility in 2001, the safety organizations considered that it was too early to extend the use of fuel assemblies using the M5® alloy to the rest of the nuclear power plant fleet. Between 2003 and 2006, EDF undertook a series of plant investigations, tests and in-depth assessments to establish the causes of M5® alloy cladding failure and to define appropriate corrective measures[810].

Since then, in light of favourable operating experience feedback, the M5® alloy has been authorized for general use across the entire French nuclear power plant fleet.

In France, EDF, wishing to diversify suppliers, loaded its power reactors with fuel assemblies supplied by Westinghouse, which already incorporated enhancements achieved by using new alloys such as Zirlo™ to limit cladding corrosion.

Loading of a few fuel assemblies supplied by Westinghouse into French reactors began in 1993. In 1995, 'prequalification' fuel assemblies comprising Zirlo™ (for the cladding, grid straps and the RCCA guide tubes) were loaded into Unit 1 of the Belleville-sur-Loire nuclear power plant and in 2003 into Unit 1 of the Paluel nuclear power plant. Significant operating experience feedback on the use of this material was at that time available from the USA, Sweden and Spain, showing that it demonstrated better in-reactor behaviour in comparison with Zircaloy-4 in terms of cladding sensitivity to corrosion and dimensional elongation. ASN then authorized the Zirlo™ alloy for general use in 1300 MWe reactors in 2006 and then, in 2007, in 900 MWe reactors (except for Fessenheim and Bugey).

Other grades of this material have, however, been tested, such as:

- Low Tin Zirlo™,
- Optimized Zirlo™, which is also a 'low tin' grade, with or without an internal liner[811] in the cladding (the liner is designed to provide protection against the initiation of stress corrosion cracking by fission products and its ductility also adapts better to stresses caused by pellet swelling during a power transient),

[810] This issue is addressed in IRSN's position paper entitled Position on Safety and Radiation Protection at Nuclear Power Plants in France in 2008, DSR report 316.

[811] In the USA, rods with an internal liner have been loaded into reactors since 1986.

– AXIOM alloys (four variants of Optimized Zirlo claddingÔ designed for better corrosion resistance).

Consequently, in 2003, EDF loaded a few fuel assemblies using Optimized Zirlo™ and the four AXIOM variants into Unit 2 at the Cruas-Meysse nuclear power plant and Unit 1 at the Paluel nuclear power plant (only the Optimized Zirlo™ cladding was tested in the latter unit). ASN then authorized the irradiation of fuel assembly reloads containing rods with Optimized Zirlo™ cladding into Unit 2 at the Belleville nuclear power plant in 2009 and then Unit 1 at the same power plant in 2012 and 2014. In 2018, Optimized Zirlo™ alloy was authorized for general use in 1300 MWe reactors.

The proportion of Zirlo™ alloy cladding in the reactors of the various series of the French nuclear power plant fleet is now significant, EDF having a strategy to diversify its fuel procurement sources; in 2018, reactors from the N4 series and 900 MWe reactors from the CP0 group (Fessenheim and Bugey) were the only ones to be exclusively loaded with assemblies supplied by Framatome.

To date and in general (for both Framatome and Westinghouse fuel), the main cause of cladding failure is explained by the presence of loose parts in the reactor coolant system. Operating experience feedback obtained between 2005 and 2015 has shown that, in France, the number of simultaneous rod cladding failures for a given reactor series (900 MWe, 1300 MWe, etc.) is at most 20 rods and that this number does not exceed five in any one reactor. The number 'five' corresponds to an assumption made for the purposes of the safety demonstration, in particular in rod cluster control assembly ejection studies (for overpressure applied to the vessel).

The above illustrates why a prudent approach should be taken to any changes to the design or fabrication of fuel assemblies, ensuring steps are taken progressively to offer adequate, relevant operating experience feedback before proceeding from one step to the next.

Finally, it is interesting to note that the designers, Framatome and Westinghouse, like other manufacturers around the world, are developing fuel rod cladding materials better capable of handling high temperatures during accidental transients, in particular with regard to core melt and cladding failure, ultimately limiting the dispersal of radioactive substances. Spurred on by the USA (DOE) and following proposals made in 2015 by the association NUGENIA[812], in 2017 the OECD selected this objective as one of the opportunities for research and innovation in the nuclear field leading up to 2050 (Nuclear Innovation 2050). Framatome and US manufacturers[813] have undertaken research work with the US Department of Energy (DOE) on the development of fuel and cladding that are more 'tolerant' in the event of light water reactor core accidents (Advanced Technology Fuel – ATF, Enhanced Accident Tolerant Fuel – EATF).

With regard to cladding, for example, Framatome is investigating chromium plating M5® alloy cladding and, in relation to fuel, adding chromium oxide to the fuel matrix.

[812] This association is described in sections 3.1.8 and 39.2.2.

[813] CEA and EDF are also conducting research in this area.

The aim is to reduce:

- release of fission gases from the fuel matrix during normal operation and accident transients,
- clad ballooning and thus the risk of cladding failure during accident transients,
- high-temperature oxidation of cladding material leading to hydrogen production.

Exploratory irradiation trials in a US power reactor (Unit 2 of the Vogtle power plant in Georgia) were scheduled starting from 2019 and others are planned in France.

For its part, Westinghouse[814] is developing a new fuel named EnCore: a number of options are being explored, such as using 'silicide' fuel[815] (U_3Si_2) which achieves better thermal conductivity than oxide type fuel, meaning that fuel temperatures can be reduced, or that silicon carbide (SiC) can be used as cladding material. Exploratory irradiation trials in a US power reactor (Unit 2 of the nuclear power plant in Byron, Illinois) were scheduled to begin in 2019.

28.3. Anomalies and significant events involving fuel assemblies

Various anomalies have affected fuel assemblies and rods since the startup of the first units of pressurized water reactors and of course led to enhanced monitoring, unloading of defective components from the core, specific inspections and the introduction of remedial measures (through design changes and other means).

Four of the most significant types of anomaly that have occurred are addressed below (other anomalies observed may be mentioned, such as cladding damage [wear] caused by loose parts[816] that jam in the grids and vibrate in the circulating reactor coolant, and failure of assembly hold-down spring screws[817]).

28.3.1. Baffle jetting

As indicated in the previous chapter (Section 27.1.1), degradation was first observed in 1981 on fuel rods located at the core periphery in the first reactors of the French nuclear power plant fleet (mainly those at the Bugey nuclear power plant), which was attributed to rod vibration induced by water crossflows resulting from degradation of

[814] Framatome is also working in this area in cooperation with CEA.

[815] Fuel already widely used for research reactors.

[816] Since 1994, the introduction of antidebris devices at the bottom of the assemblies has helped to reduce this problem.

[817] Section 9.2 of the publication *La maintenance des centrales nucléaires* (Maintenance at Nuclear Power Plants) by Jean-Pierre Hutin, EDF/Lavoisier Tec&Doc, 2016, mentions a number of fuel-assembly-related anomalies. Readers may also consult the article *Comportement du combustible des réacteurs à eau sous pression en situation de perte d'étanchéité* (Behaviour of Pressurized Water Reactor Fuel in a Cladding Failure Situation), D. Parrat, a CEA treatise on nuclear fuel.

the baffle-plate bolts at the core periphery. This type of anomaly was observed not only in France but also in other countries, in particular in the USA; in France, around twenty assemblies comprising fuel rods with cladding failure caused by baffle jetting were identified.

Initially, assemblies consisting of inert stainless steel rods were loaded at locations on the core periphery considered to be the most highly exposed but, following renewed degradation of the core baffle on Unit 2 at the Bugey nuclear power plant in 1987, the essential modification (a solution also adopted in the USA) involved reversing the direction of water flow between the baffle and the core barrel (the 'up-flow conversion') – a modification described in detail in Section 27.1.1.

28.3.2. Fretting

Following cladding failures observed through changes in reactor coolant radioactivity at Unit 3 of the Cattenom nuclear power plant (a significant event declared in 2000[818]) and others observed at 1300 MWe reactors[819], EDF carried out studies to identify the cause of these failures which, for Cattenom Unit 3 alone, affected 92 rods. Virtually all of the failed rods belonged to assemblies that had just undergone a third cycle of irradiation under the GEMMES fuel management scheme with an average assembly burnup of approximately 49 GW/t. Subsequent to irradiation, relaxation of the springs (made from Inconel 718 alloy) on the lower grid of certain assemblies (AFA 2GL and AFA 3GL assemblies designed by Framatome) was detected; this led to a phenomenon of vibrational wear followed by cladding perforation. This phenomenon, referred to as 'fretting' by EDF, proved to be a generic problem for 1300 MWe reactors (where assemblies are approximately 60 cm longer than those of the 900 MWe reactors) and the same phenomenon also affected assemblies in US reactors[820]. This demonstrated

[818] In light of changes observed in the reactor coolant radiation monitoring indicators, EDF declared that the unit was experiencing 'serious cladding failure' in September 2000; unit operation was pursued until the end of the operating cycle in progress at the end of February 2001.

[819] Cladding failures of the same type were also observed at the Penly Unit 2, Cattenom Unit 2 and Golfech Unit 1.

[820] Readers may consult, for example, the article by R. Yang, B. Cheng, J. Deshon, K. Edsinger & O. Ozer (EPRI, 2006), entitled Fuel R & D to Improve Fuel Reliability, Journal of Nuclear Science and Technology, 43:9, 951-959. From the late 1970s until the late 1980s, US (BWR and PWR) operators were very concerned about the state of their fuel. The percentage of failed assemblies sometimes rose to a significant fraction of the core. In the 1990s, while the situation was generally more satisfactory, failures were still encountered, in large part due to fretting or debris, but deposits and corrosion were also considered to be responsible for axial offset anomalies. In 1998, EPRI launched a vast programme, initially called Robust Fuel Program and then Fuel Reliability Program, that aimed to improve the situation, especially from an operational point of view (finding methods that would make it easier to identify the origin of cladding failures, ultrasound rod cleaning methods, optimization of reactor coolant chemistry, etc.). In parallel, manufacturers continued their attempts to improve fuel performance (with new cladding alloys, a protective grid called 'P-Grid' and other measures). More specifically, with regard to fuel manufactured by Westinghouse (RFA assemblies), readers may also consult the article Westinghouse 17 x 17 RFA Fuel Performance (Westinghouse/ENUSA), TopFuel Conference, 2018.

that the assembly design was not compatible with the increase in fuel burnup under the GEMMES fuel management scheme.

The failed fuel assemblies were located in an intermediate ring of the core where crossflow rates are the highest, in the lower part of the assemblies. EDF identified a mechanism capable of explaining the observed damage. Several types of phenomena are involved in fuel rod wear:

- rod hold-down in grid cells,
- changes in the mechanical characteristics of grids due to irradiation,
- crossflows and the vibrational response of the rods to the effect of these flows.

EDF concluded that the failures observed could be the result of a critical threshold being exceeded, which accelerated fretting wear, this threshold being determined, first, by thermal-hydraulic vibrational forces and, second, by the rods coming loose in the grid cells due to irradiation (hold-down capability being virtually lost at the end of irradiation).

The solution provided by the designer consisted in adding a supplementary grid above the lower grid of the fuel assemblies to enhance fuel rod hold-down in the lower part of the assemblies while maintaining compatibility with the other fuel assemblies present in the core, in particular with regard to head loss and axial hold-down. The modified fuel assemblies, designated AFA 3GLr, are equipped with reduced-width grid springs ('PRELUDE' type) designed to offset the increase in head-loss resulting from the additional grid. The first refuelling campaign using AFA 3GLr fuel assemblies took place at Unit 3 of the Cattenom nuclear power plant in 2002, accompanied by enhanced monitoring of reactor coolant activity. The same measures were then taken for the 1300 MWe reactors considered the most in need: Cattenom units 1, 2 and 3, Flamanville Unit 2, Golfech Unit 1, Paluel Unit 1 and Penly Unit 1.

Initially, the safety organizations considered that, while the addition of a grid in the lower part of the fuel assemblies was likely to offer a qualitative improvement by reducing the risk of vibrational wear on the cladding, uncertainties remained with regard to the in-reactor behaviour of the new assemblies[821], which meant that it was not possible to consider implementing this improvement on all 1300 MWe reactors, contrary to the operator's proposal, in particular for the purposes of the GEMMES fuel management scheme; AFA 3GLr assemblies were authorized for certain reactors from 2002 onwards, this authorization then being extended to all 1300 MWe reactors once satisfactory operating experience feedback had been obtained.

With regard to 900 MWe reactors, EDF considered that the risk of vibrational wear was lower. This is because, although the lower part of a 900 MWe reactor assembly

[821] EDF conducted 1000 h of loop tests (called 'HERMES-P' under temperature, pressure and flow conditions representative of those prevailing in normal reactor operation) involving AFA-2GL and AFA-3GLr assemblies, where some of the grid springs had previously been subjected to plastic deformation to simulate their relaxation by irradiation. The conclusion drawn from these tests, however, was that a comparative interpretation of the wear results for the two types of fuel assembly did not provide a straightforward outcome, but that the new design had no negative effects.

is more sensitive to flow-induced vibrations (given that the natural frequency of a 900 MWe reactor fuel rod is lower than that of the 1300 MWe reactor fuel rods[822]), flow rates in 900 MWe reactors are lower than in 1300 MWe reactors (with axial velocity 10% lower and crossflow velocity 30 to 40% lower). The safety organizations, however, considered that it was difficult to completely rule out fretting wear in 900 MWe reactors, especially since the CYCLADES fuel management scheme (implemented for the Fessenheim and Bugey reactors) would lead to higher maximum burnup than for the 1300 MWe reactors; however, operating experience feedback did not reveal any cladding failures due to fretting in 900 MWe reactors.

Cladding wear and perforation due to fretting have also been observed on fuel assemblies supplied by Westinghouse that have been irradiated in the 1300 MWe reactors of the French nuclear power plant fleet. In order to overcome these wear problems, EDF gradually loaded the reactors (including 900 MWe reactors for fuel assemblies using the Zirlo™ alloy) with assemblies supplied by Westinghouse, which are equipped with an additional grid (the ‘P Grid’) at the bottom of the assembly to limit the risk of vibrational wear on cladding.

A large number of fuel assemblies used in the nuclear power plant fleet now have an additional grid at the bottom of the assembly.

Finally, it should be noted that the radiochemical specifications currently in force for reactor coolant would no longer authorize a reactor in the nuclear power plant fleet to operate with a rate of cladding failures equivalent to that reached in 2000 at Unit 3 of the Cattenom nuclear power plant.

28.3.3. Events encountered during handling operations

Problems may occur during fuel assembly handling operations (loading/unloading assemblies into/from the core). They deserve special attention because they can result in damage to assemblies, in particular deterioration of the fuel rod spacer grids, by tearing off pieces of grid straps[823], which may become loose parts.

The event that occurred in September 2008 at Unit 2 of the Tricastin nuclear power plant is described below[824].

[822] The lower grid on fuel assemblies in 900 MW reactors is located at a higher elevation than that of the fuel assemblies in 1300 MWe reactors.

[823] The grids, which ensure that the rods are uniformly spaced from one another throughout the lifetime of the fuel assembly, consist of straps fitted with bow springs.

[824] See IRSN’s Position on Safety and Radiation Protection at Nuclear Power Plants in France in 2008, DSR report 316, as well as the report entitled *Rapport de l’Inspecteur général pour la sûreté nucléaire et la radioprotection – 2008* (Report of the Inspector General for Nuclear Safety and Radiation Protection – 2008), P. Wiroth (EDF), Section 19.1. It should be noted that two other instances of assemblies engaging the upper internals were observed in August 2009 at Unit 1 of the Gravelines nuclear power plant and in November 2009 and February 2019 at Unit 2 of the Tricastin nuclear power plant.

When lifting the upper internals from the vessel of a pressurized water reactor during an outage, a closed-circuit TV inspection is conducted under the lower face of the upper internals before they are completely lifted out, to check that no control rod assemblies or fuel assemblies have engaged the internals.

On 8 September 2008, during an outage at Unit 2 of the Tricastin nuclear power plant, pictures from the TV inspection revealed that two fuel assemblies located at the core periphery (positions B08 and C08) had engaged the upper internals (see Figure 28.4). The risk involved in this state was that one or both of the assemblies would disengage and fall into the core, possibly resulting in cladding rupture with dispersal of fission products in the water of the reactor pool followed by release into the air inside the reactor building.

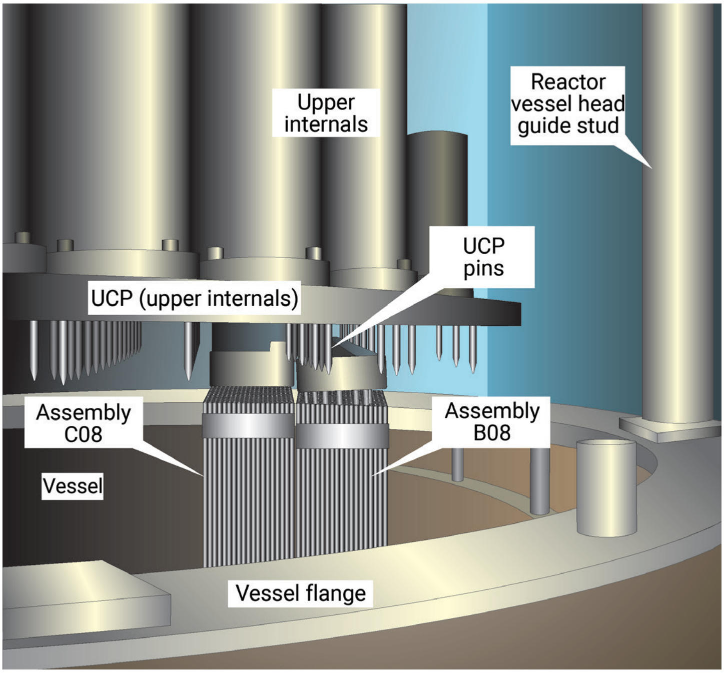


Figure 28.4. Schematic diagram of the two fuel assemblies that engaged the upper internals (UCP: upper core plate). IRSN.

The two assemblies in question had been lifted to three quarters of the core height.

The facility operator immediately decided to evacuate the reactor building. To prevent one or both of the fuel assemblies from falling, it was then decided to secure them in place by the top nozzle using a dedicated tool. Once the assemblies had been secured, a hydraulic jack attached to the special tool was used to disengage the top nozzles from the upper internals. The upper internals were then lifted and set down on their stand. Finally, on 27 October 2008, the assemblies in question were removed from the reactor core and transferred to the fuel building.

Subsequent investigation revealed the presence, on the lower core plate (LCP), of several balls (4.7 mm in diameter) that had not been detected during previous outages (in 2006 and 2007), mainly because of the turbidity of the water and poor lighting. These balls came from the damaged ball bearing cage of a tool used for refuelling during 900 MWe reactor outages. Based on these findings, EDF deduced the following scenario for the 8 September 2008 event: in 2007, a few balls originating from the damaged cage became lodged under the base of the fuel assemblies, in positions A08 and B08. They caused significant gaps (between 12 mm and 15 mm) to be formed between the fuel assemblies. When the upper internals were refitted, since several centring pins on the upper core plate (UCP) were no longer perfectly aligned with the bore holes in the top nozzle of the assemblies located in positions B08 and C08, the forces generated by friction tore away some material from the edge of the bore holes. The pins entering the bores holes containing this surplus material became jammed.

Other instances of fuel assemblies engaging the upper internals occurred in 2009 at Unit 2 of the Tricastin nuclear power plant and Unit 1 of the Gravelines nuclear power plant. The analysis and handling of these events in 2008 and 2009 led EDF to formalize procedures for all the reactors in the nuclear power plant fleet, to be followed in the event of fuel assemblies engaging the upper internals during lifting (securing the assembly or assemblies in question, disengaging the upper internals and transfer of the relevant assemblies to the fuel building). Furthermore, the condition of the bore holes, the clearance between fuel assemblies once all the assemblies have been reloaded, and determining the absolute position of the assemblies in the core are now subject to systematic and thorough visual inspection in order to prevent this type of event.

28.3.4. Lateral deformation of fuel assemblies interfering with RCCA drop

Fuel assemblies undergo lateral deformation[825] during irradiation in the reactor under the combined effects of the hydraulic forces exerted by the water circulating in the reactor core, the mechanical forces applied by the upper core plate on the top nozzle to hold them in position, irradiation and temperature (changes in mechanical characteristics). Fuel assembly design, in particular the thickness and material of the guide tubes (which have an influence on the rigidity of the assembly), together with assembly position in the core, are decisive factors in deformation. Observable during measurements performed once the assemblies have been unloaded from the core, deformation is unknown when the reactor vessel is closed. However, major deformation may slow down rod cluster control assemblies when they are dropped, or even prevent them from dropping completely, while RCCA drop time and complete insertion are central assumptions in safety studies. This is why the facility operator periodically measures RCCA drop time in the reactor to check for compliance with these assumptions, in accordance with general operating rules.

[825] Into a C shape (banana), S shape or even W shape (double S).

Lateral deformation of fuel assemblies may also cause operational problems during core unloading operations.

Operating experience has shown that fuel assemblies may undergo different types of lateral deformation (see Figure 28.5). The situation improved in the 2000s once preventive measures had been introduced and more rigid assemblies were used. However, new difficulties related to excessive lateral fuel assembly deformation were observed in the 2010s, affecting Unit 2 at Chooz B (N4 series reactor, ALCADE fuel management scheme) and Unit 2 at Nogent-sur-Seine (1300 MWe reactor, GALICE scheme) nuclear power plants.

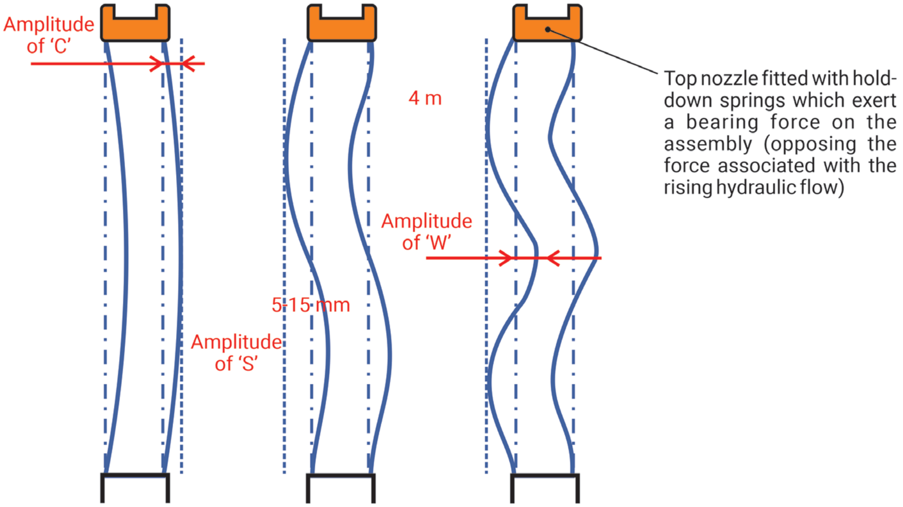

Amplitude of 'C'
4 m
Top nozzle fitted with hold-down springs which exert a bearing force on the assembly (opposing the force associated with the rising hydraulic flow)
Amplitude of 'W'
5-15 mm
Amplitude of 'S'

Figure 28.5. Illustration of lateral assembly deformation, indicating the order of magnitude of the deformation measured 'outside the core'. IRSN (source EDF).

The lateral deformations of particular concern on fuel assemblies observed on completion of the 18th operating cycle of the Nogent Unit 2 and the subsequent measures taken by EDF are described in detail below[826].

The singular situation of this unit is related to implementation of the GALICE fuel management scheme, in which a smaller number of new assemblies is introduced on each reload than in the GEMMES fuel management scheme implemented in all the other 1300 MWe reactors. As a consequence of the difficulties encountered, EDF definitively decided to cease efforts to implement the GALICE fuel management scheme (this scheme had only been implemented at Unit 2 of the Nogent-sur-Seine nuclear power plant). Furthermore, from 2013 onwards, EDF decided to reload Unit 2 of this power plant, for its 20th cycle, with new assemblies equipped with new guide tubes

[826] See IRSN's Position on Safety and Radiation Protection at Nuclear Power Plants in France in 2013 (IRSN public report DG 2014-00001) and Safety and Radiation Protection at Nuclear Power Plants in France in 2015 – IRSN's Position (IRSN public report DG 2016-00004).

(manufactured using a new material characterized by lower irradiation creep) to reduce lateral deformation (their use had previously been authorized in 2012 for Unit 2 at the Chooz B nuclear power plant).

These measures were considered satisfactory by the safety organizations, but subject to enhanced monitoring of RCCA drop time and additional mid-cycle tests. In 2014, performance of these tests during the 19th unit operating cycle revealed deterioration in drop-time results, which obliged the facility operator to carry out monthly tests to check that fuel assembly deformation was not jeopardizing reactor trip availability. In light of the considerable increases in drop time for certain RCCAs during the cycle and incomplete insertion of five RCCAs, EDF finally decided to shut down the unit three months before the planned outage date and defuel the core.

During the 20th operating cycle of Nogent Unit 2, enhanced fuel assembly monitoring again revealed incomplete insertion of a rod cluster control assembly. This event occurred in March 2015, while the reactor refuelling outage was not scheduled until September of the same year. EDF decided to carry out an in-cycle shutdown, unload two fuel assemblies associated with RCCAs showing an abnormal drop time and 'repair' them to prevent renewed rod drop time anomalies during the second part of the 20th cycle.

Before pulling these two severely deformed assemblies, the facility operator had to unload two neighbouring assemblies in order to facilitate removal of the two incriminated assemblies. This procedure made it possible to limit fuel assembly handling operations (which always involve the risk of damage to grids), the rest of the core remaining in place. The facility operator then carried out an unprecedented 'assembly skeleton replacement', which involved transferring the 264 fuel rods from a deformed assembly into a new, undeformed assembly structure. This operation was carried out in the spent fuel pool using a dedicated tool known as STAR (see Figure 28.6). The 'repaired' fuel assemblies were then loaded into the reactor core in their initial positions. This operation, authorized by ASN following an IRSN assessment, lasted several days.

ASN requested that EDF test RCCA drop time at regular intervals, at least once every 60 days, to check compliance with specified limit values and ensure that rods did not jam up to the end of the 20th cycle. The limit values were not exceeded nor did any rods jam during the second part of the 20th cycle during the four drop-time tests carried out following reloading of the two 'repaired' assemblies (the GALICE fuel management scheme was then abandoned in favour of the GEMMES scheme).

In general, lateral deformation of fuel assemblies is the result of complex causes that remain poorly understood, both in France and in other countries, particularly because deformation cannot be measured in a reactor vessel, especially when the reactor is in operation. Assembly deformation is monitored by EDF at reference reactors in which greater levels of deformation may be anticipated. Monitoring is conducted using the DAMAC unit mentioned in Section 28.1.2, following unloading of the fuel assemblies,

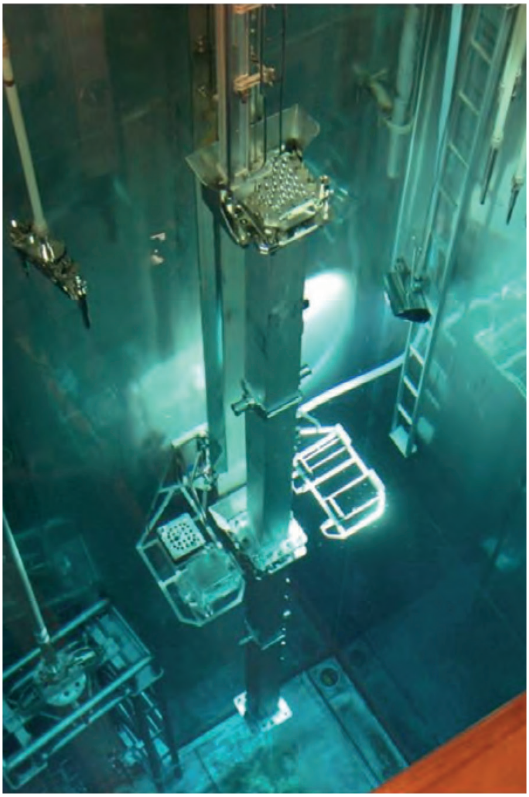


Figure 28.6. View of STAR, the 'assembly skeleton replacement system' in the spent fuel pool. EDF.

when they are transferred to the spent fuel pool. Even in the absence of major deformation requiring corrective action, all cores exhibit deformations that may lead to various consequences. This deformation causes variation in the thickness of the water layers present between the fuel assemblies, and the impact of this variability in terms of neutron physics, thermal-hydraulics and fluid mechanics must be taken into account in the safety demonstration, which was what ASN wanted EDF to investigate, in particular in 2015 with the prospect of the upcoming periodic reviews for the fourth ten-yearly outage of the 900 MWe reactors. In 2017, using available measurements of lateral assembly deformation carried out during refuelling and a simulation model, EDF finalized a method for estimating the distribution of water layers in a core and then evaluated the consequent impact in terms of neutron physics, thermal-hydraulics and fluid mechanics.

Chapter 29
Facility Compliance

29.1. Introduction

It is the responsibility of nuclear facility operators to appropriately document the state of safety for each facility throughout the different stages of its lifetime. This means that facilities must comply with 'baselines'[827], mostly defined at the design stage. However, during construction or due to operating activities or the effects of ageing, the actual condition of facilities may differ from the condition stated in the safety demonstration.

Certain equipment items must be able to function in an earthquake or accident situation, i.e. when affected by mechanical stresses or under specific ambient temperature, pressure and irradiation conditions; these equipment items must therefore undergo 'qualification' prior to commissioning. Qualification consists of demonstrating the ability of equipment to perform its functions under these conditions (see Chapter 7). If any item of equipment no longer satisfies qualification conditions, then it cannot perform its functions fully and the facility is no longer compliant. In order to maintain a satisfactory safety level, the operator must therefore identify, analyse and correct any deviations from compliance.

[827] For this concept, see Chapter 2 (organization of safety control) and Chapter 30 (periodic reviews).

29.2. Detection and treatment of compliance deviations for pressurized water reactors in the nuclear power plant fleet

In the 2000s, the checks and inspections carried out during the second ten-yearly outage[828] on 900 MWe reactors revealed a large number of deviations from the design baselines for these reactors. By their nature, these deviations were often generic, i.e. they affected several reactors, possibly located at different sites, making them more complicated to rectify. In some cases rectification could not be achieved in strict compliance with the general operating rules. From 2001, EDF therefore decided to consider them as a particular family of deviations, known as 'compliance gaps', and it set up a special process to deal with them in which the time allowed for rectification was adapted to reflect the deviation's importance from a safety point of view.

Compliance gaps can occur in particular as a result of:

- the facility's inherent shortcomings (design, manufacture, assembly),
- maintenance operations,
- retrofits and upgrades,
- equipment ageing,
- anomalies in studies supporting the safety demonstration.

Baseline changes involving equipment, operating rules and procedures, etc., particularly during periodic reviews, must be implemented appropriately and in a timely manner.

This chapter describes the process set up by EDF to deal with compliance gaps and presents several typical examples.

29.2.1. Process for handling compliance gaps

EDF's process for handling compliance gaps detected at nuclear power reactors consists of four steps:

▶ Detection – Discovery of the compliance gap

Deviations are detected by nuclear power plant management or by engineering centres. If a compliance gap is potentially generic, it is handled by EDF's corporate engineering services. Depending on the urgency or importance of the gap, EDF may decide at this stage to implement compensatory measures to remedy all or some of its consequences.

[828] See Chapter 30 for the ten-yearly reactor outages and the associated periodic reviews.

▶ Characterization of the compliance gap

Characterization consists in assessing the safety consequences of the gap and ascertaining whether it is generic. Subsequently, EDF can determine the degree of urgency to be applied in its management strategy, depending on the risk induced by the gap. If, following characterization, the safety consequences are found to be significant, a significant safety event is declared (based on the criteria given in Chapter 21).

▶ Definition of the management strategy

Based on the characterization results, EDF defines a management strategy that may consist in:

- maintaining the facility as it is,
- defining compensatory measures to make up for the compliance gap until permanent measures can be implemented,
- defining an operational process to remedy the gap and setting a deadline to complete this process,
- bringing the affected reactors to a safe state if the potential safety consequences are considered unacceptable.

▶ Implementation of corrective actions

The facilities are brought back into compliance. Depending on the safety impact, this may be achieved immediately or during scheduled refuelling outages or ten-yearly inspection outages.

Throughout the process, EDF keeps the French Nuclear Safety Authority (ASN) and IRSN informed. IRSN assesses the handling of compliance gaps at each stage of the process and can make recommendations.

Depending on the number of compliance gaps detected and the remediation deadlines set for each, reactors can be affected by several compliance gaps at any given time. Consequently, since 2011, each nuclear power plant operator must keep a log of all current compliance gaps at the facility and continuously update this list so that it has an exhaustive overview of the state of the facility. It must assess the combined safety consequences of all the compliance gaps simultaneously affecting the reactor if they cannot be rectified quickly. To make this assessment, EDF's central services carry out a cumulative analysis of the generic compliance gaps for each series or reactor type, making a distinction for specific cases such as Fessenheim and Bugey (CP0), the reactors in programme contracts CP1 and CP2, etc. This analysis defines a virtual reactor with all the compliance gaps likely to affect the corresponding series or reactor type. Analyses of the combined compliance gaps specific to each reactor are then carried out, based on the generic analysis. This study determines whether it is necessary to review the original deadlines for addressing certain compliance gaps or to implement additional compensatory measures.

29.2.2. Examples of compliance gaps

Some examples of compliance gaps found at reactors in the French nuclear power plant fleet are presented below, illustrating the different causes and natures described above. Certain other events, which also constitute compliance gaps, have been mentioned in previous chapters. Further information is provided here regarding the handling of abnormal vibrations in low-head safety injection pump motors and containment spray system pump motors, as well as rotor lift in these pumps, which was discussed in Chapter 19 on startup testing of pressurized water reactors.

29.2.2.1. Compliance gap in electrical connection boxes qualified for accident conditions

In 2003, when Unit 2 at the Penly nuclear power plant was operating at power, an insulation defect was found in the electrical connection boxes of two reactor containment isolation valves. This defect was caused by inadvertent spraying due to a leak in the steam generator feedwater system. The investigations carried out following this event showed that some electrical cables had nicks in the insulation that exposed the copper of the wires, and that the insulating sleeves were too loose; these anomalies were due to poor quality work by electricians and inadequate inspecting.

If emergency procedures were to be applied, the actuators energized via these boxes would be necessary to bring the reactor to a safe shutdown state. Accordingly, they were qualified for accident conditions. The anomalies observed in the cables and insulation therefore compromised the electrical insulation requirement for the affected connections, thereby constituting compliance gaps.

Subsequent inspections found similar anomalies in 57 of the 122 electrical connection boxes of this type in the Unit 2 building at the Penly nuclear power plant.

In the first quarter of 2004, inspections carried out at the Gravelines and Flamanville nuclear power plants revealed that these anomalies were generic. Similar anomalies were also discovered in instrumentation cables.

As a result of these findings, EDF prepared an investigation programme to inspect, in particular, the boxes most important to safety. The inspections and rectification work continued until 2007 across the entire nuclear power plant fleet. At some reactors it was even necessary to resume the inspections in 2008 following the detection of anomalies not found earlier.

To prevent further anomalies, EDF introduced a baseline whereby the actions implemented during the rectification process were made permanent, which involved raising the awareness of all those concerned, updating the requirements for maintaining equipment qualification, and writing corporate-wide maintenance procedures accompanied by summary notes for those responsible for inspection and surveillance.

29.2.2.2. Failure in the seismic resistance of metal floors in electrical and auxiliary buildings of 900 MWe reactors (CPY series)

In 2005, as a result of preparatory work for the implementation of changes related to fire protection, EDF found compliance gaps concerning the types of anchor bolts used to hold down metal floors in the electrical buildings of the Chinon B, Saint-Laurent-des-Eaux B and Dampierre-en-Burly reactors. It began work to remedy these compliance gaps and continued its investigations to establish whether the deviations were generic.

Following a Complementary Investigation Programme (see chapters 27 and 30), which included checks of all non-fire-resistant metal floors and all metal floors with fire-resistant padding on their underside in the electrical and auxiliary buildings of the 900 MWe reactors under the CPY programme contract, EDF indicated that it could not guarantee that the floors could withstand a MHPE[829] in the case of 17 reactors or a seismic margin earthquake (SME) in the case of the other reactors, since the anchor bolts of these floors were only partially characterized. Conservatively, it could be anticipated that, in an earthquake situation, all these floors could fall due to a domino effect, causing the loss of all the equipment on or below the falling floor and, with it, the loss of the measuring capability necessary to obtain nuclear steam supply system parameters and the ability to actuate certain devices required in accident situations.

Initially, EDF installed temporary support column bracing equipment to guarantee that each floor could withstand MHPE conditions. Later on, it undertook permanent remediation work on all the affected metal floors to guarantee their ability to withstand a seismic margin earthquake.

29.2.2.3. Risk of containment sump screen blockage

Containment sumps are provided to collect water from the reactor coolant system in the event of a break as well as water from containment spraying. As explained in Chapter 9 on loss-of-coolant accidents, this water is ‘recirculated’, i.e. it is returned to the containment spray system, which cools the water and sends it to the safety injection system, which in turn sends it to the core for fuel cooling.

If a reactor coolant system break occurs, the water jet spurting from the break produces a large amount of debris, mainly from damage to the insulation and other materials near the ruptured pipe. The dust and debris in the air or deposited on structures inside the reactor building is washed away by the water sprayed inside the containment. This debris is carried away in the water by gravity into the lowest part of the containment and accumulates upstream of the sump strainers. It may then form a porous bed, which can affect the performance of the recirculation pumps downstream of the strainers.

[829] Maximum Historically Probable Earthquake (see Section 12.3).

The strainers were originally designed to prevent the risk of clogging and restrict the passage of debris into the downstream systems and the core.

However, operating experience feedback and the acquisition of knowledge on this subject (see Section 9.1.4) have raised questions regarding the effectiveness of strainer design. In December 2003, EDF told the safety regulator that it could not exclude the risk of the sump strainers clogging in accident situations involving a reactor coolant system pipe break.

French nuclear power reactors were fitted with strainers having different mesh sizes that varied from one series to another. They were vertical panels installed in the sumps in a circumferential arrangement. Based on knowledge acquired through research and development on the risks of sump strainer clogging[830], two types of changes were decided in 2004 and were then implemented:

- removal of the Microtherm® insulation, which can generate very small particles, which is unacceptable in terms of the risk of sump strainer clogging,
- replacement of the strainers with new strainers featuring a significantly larger surface area (up to 48 times that of the previous strainers).

Nonetheless, the effectiveness of cooling the core by recirculating water from the sumps in a loss-of-coolant accident was not fully demonstrated, because some key questions remained unanswered (see sections 9.1.4 and 30.5.3).

The solution adopted for the EPR is presented in Section 18.2.4.

29.2.2.4. Anomaly found in engines of emergency and SBO diesel generators for 900 MWe reactors

A compliance gap involving the connecting rod big-end bearings in emergency and SBO diesel generators at 900 MWe reactors was the cause of many diesel engine failures.

The connecting rod big-end bearings (see Figure 29.1) are half-ring-shaped parts that act as the interface between the connecting rod big end and the engine crank pin; they are made of steel with a copper and lead alloy anti-friction coating.

The original manufacturer had stopped making bearings in 2003; the diesel engine manufacturer then contracted with another manufacturer to make the same parts. The first series of bearings made by the new manufacturer (the 'first-generation bearings') was then installed from 2006 in several diesel engines at 900 MWe reactors during routine maintenance operations. But in 2008 and 2009, several engine failures occurred. An assessment of the bearings revealed rapid deterioration due to a generic manufacturing defect (areas where the anti-friction coating was slightly too thin),

[830] See Chapter 5 of Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

which could lead to melting of the metal that the bearings were made from at certain points. EDF and the engine manufacturer had not thought it necessary to conduct qualification tests on the new manufacturer's parts, which were supposedly manufactured identically to the old ones.

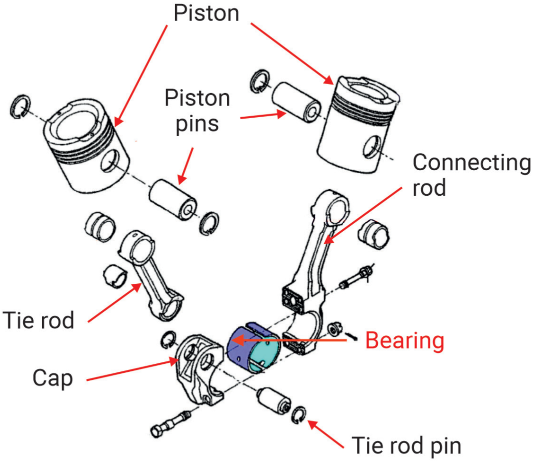


Figure 29.1. Diagram showing the location of the connecting rod big-end bearings (in blue). IRSN.

Under these circumstances, the manufacture of a second series of bearings (second-generation bearings) was launched in 2009; the defect in the anti-friction coating was corrected. The second-generation bearings underwent factory testing in an engine identical to those installed in the nuclear power plants, where the number of engine startups performed was equivalent to ten years of operation. Because the engine manufacturer considered that these tests showed that the new bearings behaved correctly, they were installed in place of the first-generation bearings.

However, in October 2010, two engines fitted with the new bearings were affected by failures, and inspections of two other engines again revealed abnormal wear of the new bearings. To maintain an acceptable level of engine reliability, enhanced monitoring and maintenance was implemented by EDF as a preventive measure.

In spite of these measures, since April 2011, second-generation bearings in five engines have had to be replaced for reasons of premature wear. In one of these engines, the bearings have even been replaced three times. Because the second-generation bearings are therefore not a permanent solution, EDF carried out detailed investigations in 2011. It concluded that the rapid wear of the bearings could be caused by insufficient lubrication due to a geometrical deviation. In 2012, EDF and its industrial partners therefore defined a new bearing, known as '2 bis', in which the geometrical differences between the original and second-generation bearings were corrected. The 2 bis bearings were qualified and their installation in engines at nuclear power plants began.

29.2.2.5. Temperature resistance fault in the high-head safety injection pumps

Following the 2003 and 2006 heatwaves, requirements to protect nuclear power plants from high ambient temperatures (the 'extreme heat baseline') were reviewed. During the study carried out in this context by EDF, it was found that there were inadequacies in the design of systems for cooling buildings containing the high-head safety injection pumps of 900 MWe reactors (CPY series). In some accident situations, the temperature in these buildings could temporarily reach values at which the pumps were no longer guaranteed to work properly. These temperatures could affect the high-head safety injection system's ability to perform its core cooling function in these accident situations.

The analysis carried out by EDF showed that the part of the pump that was the most sensitive to ambient temperature was the thermostatic valve that regulates the lubricant temperature. Overheating on the valve control component could cause the valve to lock in the position that sends the lubricant to the air cooler bypass line and consequently cause the pump to fail due to heating of the lubricant.

Initially, in 2008, to ensure the pumps were fully operational again in accident situations, EDF replaced these thermostatic valves with valves qualified for higher temperatures, similar to those in the same system of the 1300 MWe reactors. However, just after these valves were installed, even though the operating tests on the first modified pump were judged satisfactory, malfunctions occurred at the Dampierre-en-Burly, Blayais and Tricastin nuclear power plants. These malfunctions, due to the rupture of part of the valve control stem, caused an air cooler bypass and therefore led to a rise in temperature of the lubricant and the lubricated components. Expert investigations carried out showed that pressure fluctuations in the system, induced by the operation of the pre-lubrication pump, caused the malfunctions observed.

As a result of this finding, EDF quickly took measures to mitigate failure of the new thermostatic valves and the subsequent impact on safety. These measures included 'overriding' the control unit of the thermostatic valve on one safety injection pump per reactor to direct the lubricant flow to the air cooler, restricting the operating time of the pre-lubrication pumps, and ensuring enhanced monitoring of safety injection pump operation. EDF later replaced the pre-lubrication pumps with pumps that caused less vibration.

29.2.2.6. Mixed lubricants in equipment required for accident situations

From the 1980s to 1990s, inappropriate lubrication leading to mixing of different lubricant references, the use of lubricants not compliant with the manufacturer's instructions, and omitting to lubricate new equipment or perform periodic top-ups, were regularly observed by EDF (an example is given in Section 26.5.2). Inappropriate lubrication can affect redundant equipment in a system important to safety and therefore constitutes a potential common-cause failure mode. Lubrication of equipment that must operate in accident situations (referred to as 'qualified' in the rest of this section), such as the safety injection system (SIS) and containment spray system (CSS), etc. is therefore a sensitive issue.

At the end of the 1990s, a lubrication policy for motor-driven pumps was established by EDF, which reduced the frequency of lubrication-related incidents. However, events in the 2000s showed that the subject required ongoing attention.

▶ Mixed lubricants observed in qualified valve servomotors

Two different lubricants, both qualified for accident conditions, were used to lubricate qualified valves. One lubricant (lubricant A) was for lubricating the electric servomotor for a valve, while another (lubricant B) was for lubricating the valve itself (stem nut, stem thrust bearing housing, etc.).

In 2008, during preventive maintenance at the Nogent-sur-Seine nuclear power plant, a worker noticed the presence of lubricant B in the grease fittings of four qualified servomotors that should only have contained lubricant A. The same problem was then discovered in 20 other servomotors: lubricant B, normally intended for valves, had been applied to the servomotor. This meant that there was a 'non-qualified' mixture of the two lubricants in the servomotors. Although both lubricants were qualified and their respective ingredients (oils and thickeners) were not incompatible, when mixed together in variable proportions, they could not be considered as 'qualified'. The resulting mixtures could lose their lubricating properties in ambient accident conditions and cause unavailability of the equipment in question.

Inspections carried out at all nuclear power plants showed that this was a generic compliance gap. Restoring compliance entailed dismantling the servomotors to clean them and replace the lubricant. Depending on the nature of the mixed lubricants and the importance of the servomotor's role in safety, compliance was restored immediately or during maintenance operations at a later time.

▶ Mixed lubricants in motor-driven pumps in the residual heat removal system (RHRS) of the shutdown reactor

When the qualified lubricant used for the bearings of motor-driven pumps in the RHRS was no longer manufactured, EDF replaced it with an equivalent qualified lubricant that met the same lubrication specifications. It decided, for the motor-driven pumps in question, to replace the initial lubricant by means of 'flushing', which consists of injecting, in a single shot, a quantity of lubricant equal to one and a half times the calculated volume of free space between the bearings in each bearing housing of the pump or motor.

However, lubrication by 'flushing' does not completely flush out the old lubricant. It therefore leads to the formation of a mixture of two lubricants in unknown proportions. Although the guide to operation and maintenance of RHRS pumps prohibited the mixing of lubricants with different references, EDF considered that the process was acceptable in this case because both of the lubricants were qualified and the supplier of the new lubricant had confirmed its compatibility with the old one.

Following a systematic inspection of the lubrication of motor-driven pumps at all nuclear power plants, non-compliant lubrication was found in 29 motor-driven pumps out of a total of 116. Because EDF could not demonstrate qualification of the mixture of these two lubricants, it declared a generic significant safety event in 2009. Further tests and analyses subsequently carried out by EDF demonstrated that the lubricant mixture could withstand accident conditions. However, without waiting for the results of these tests, EDF brought several motor-driven pumps back into compliance on a preventive basis by removing the moving parts of the pump and replacing them with new moving parts treated with the new qualified lubricant.

29.2.2.7. Flow imbalance between safety injection lines of 900 MWe reactors

The 900 MWe reactors have three water circulation loops for core cooling. Any of these three loops could undergo a break. Part of the water injected by the safety injection system (SIS) would then be discharged through the break. To limit this loss, the flows sent into the safety injection lines are balanced during preliminary tests conducted prior to reactor startup. For this purpose, each line is equipped with a needle valve for adjusting its flow. In the safety demonstration, a maximum imbalance of 6%, including uncertainty, is assumed. Compliance with this criterion is periodically checked during tests carried out during refuelling outages, based on measurements of loss of pressure due to friction in a straight pipe ('Barton tube' measuring principle) in each safety injection line. If there is an imbalance between the safety injection lines, the needle valves are adjusted.

When the 900 MWe reactors were designed, a technology was chosen for measuring the flow in the SIS lines without any particular requirements as regards measurement uncertainty. The uncertainty associated with these measurements was set by the measuring device manufacturer at a fixed rate of 1%, compatible with the maximum imbalance of 6% adopted for accident studies. In 2007, as part of a technical investigation carried out by IRSN regarding uncertainty in measurements taken during periodic tests, EDF was asked to substantiate the estimated uncertainty for this flow measuring device. It became apparent that the uncertainty associated with the device had been substantially underestimated, casting doubt on whether the safety criterion for the maximum acceptable flow imbalance between safety injection lines was met; the consequences of failure to meet this criterion could be greater fuel degradation than expected because of insufficient cooling. The measuring device therefore had to be modified.

Installing a permanent solution suitable for all the 900 MWe reactors required major work; it would therefore take a long time to prepare for and carry out the changes. This was incompatible with the need to check and, where necessary, rectify imbalances between the injection lines as quickly as possible. For this reason EDF first installed a temporary solution that consisted of replacing measurement of the flow with measurement of the fluid velocity using ultrasonic probes in contact with the pipes, for which it was not necessary to dismantle the pipes. At the end of 2012, all the

900 MWe reactors had been checked using this device. At most of them, the balance criterion was not met and the needle valves therefore had to be adjusted.

29.2.2.8. Anomaly in CATHARE software modelling of natural circulation in the upper part of the vessel

If the reactor coolant pumps shut down, the forced circulation of water in the reactor coolant system stops and natural circulation begins. In this situation, the aim of reactor operation is to reach a safe state by cooling the reactor coolant system using the steam generators and by depressurizing the system. Because there is little water circulation under the vessel closure head, this area remains hot, which delays depressurization.

In 2010, EDF noticed that the modelling of the area under the vessel closure head in the CATHARE[831] thermal-hydraulic simulation software could not take into account the phenomena observed (formation of a steam bubble under the vessel head) in real situations (tests, incidents). These modelling shortcomings could slow down or even change the reactor's shutdown transients in the long term, leading to an increase in the calculated radioactive releases, or the definition of an inappropriate operating strategy. However, the first conclusions of EDF's analysis of this representation error showed that the impact on safety studies should be low, except in the case of a steam generator tube rupture (SGTR).

EDF proposed to rectify this anomaly before the next ten-yearly inspection outage of the first unit in each reactor series; it immediately analysed the emergency operation procedures up to the fallback state for the different transients in order to make the adjustments required to ensure that the procedures were robust enough to handle a steam bubble under the reactor dome.

29.2.2.9. Vibrations and rotor lift on engineered safety motor-driven pump units

It was explained in Section 19.5 that, in the 1980s, anomalies (vibrations, rotor lift) were identified affecting the SIS and CSS engineered safety features in 900 MWe and 1300 MWe reactors and that a number of measures were taken to rectify them.

However, for some 900 MWe reactors under the CPY programme contract, vibration episodes continued to be observed during periodic tests. In 1996, at the Gravelines nuclear power plant, two motors that presented vibration levels higher than the shutdown criterion during periodic testing had to be replaced. This also prompted EDF to readjust the tie rods of the engineered safety pump motors in 900 MWe reactors.

In 2004 and 2005, EDF conducted a test campaign on pumps at the premises of manufacturer Guinard to find the possible causes of vibrations in these motors and

[831] The CATHARE simulation software is a thermal-hydraulics code developed by CEA and financed by EDF, Areva (later Framatome), CEA and IRSN; among its features is the ability to simulate flows in the reactor coolant system and the secondary system (see Chapter 40).

measure their impact. The tests were performed at full scale. They revealed a risk of rotor lift in the pumps installed in 900 MWe reactors when they take in hot water and showed that the tie rods installed previously were not efficient enough. Double-acting upper bearings were installed, as was the case for these pumps at the 1300 MWe reactors. The tie rods of the motors considered vulnerable in 900 MWe reactors were replaced by stiffener feet (3 or 6, depending on the pump). However, this did not have the desired effect on the engineered safety pump vibration levels at the 900 MWe reactors (CPY). A study showed that the stiffness of the floors on which the motors were resting also played a part, since the natural frequency of the reactor floors was similar to the rotation frequency of the motors. Installing stiffening posts under the floors did not have the desired effect either.

In 2006, the question of the engineered safety pumps' qualification for accident conditions was discussed again at a meeting of the Advisory Committee for Reactors; this caused EDF to carry out a general review of the situation at all reactors, covering 2300 pumps, and to undertake an additional qualification programme of the motor-driven pumps in the low-head safety injection system and containment spray system at 900 MWe reactors, based on tests (in the EPEC[832] experimental loop), measurements, recordings and equipment assessments, in order to find a durable solution. The programme did not identify any new generic improvement measures other than those that had already been tried.

Reducing pump vibrations had to be dealt with on a case-by-case basis. For example, the installation of extra weights to reduce the motor's natural frequency by a few hertz so it did not match that of the floor, was one of the measures taken to restore satisfactory vibration levels.

[832] *Essais des Pompes en Eau Chaude* (hot-water pump tests). This loop, which previously belonged to EDF and Framatome, is now owned by EDF. In the early 2010s it was transferred from the French Naval Construction Directorate (*Direction des constructions navales, services et systems*, DCNS, which became Naval Group in 2017) at the Nantes-Indret site to the Grenoble Fluid Mechanics Research Centre.

Chapter 30
Periodic Reviews

30.1. Introduction

Nuclear facility safety is never fully achieved and requires constant efforts to continuously incorporate improvements inspired by new knowledge and operating experience. From the time the very first reactors were commissioned, increasingly stringent safety requirements have been applied to the design, construction and operation of new reactors. Periodic reviews are conducted on existing facilities to check their compliance with applicable safety requirements and baselines, reassess the safety levels achieved, look for ways to improve safety and assess whether facility operation is acceptable.

Periodic reviews are not only common practice at French nuclear power plants since the late 1970s, they are now required under French regulations. In France, a decree passed in 1990, amending the 1963 decree on nuclear facilities, defined, for the first time, a specific regulatory framework for what it called 'safety reviews': "The ministers in charge of industry and major technological risk prevention can jointly require the operator to conduct a safety review of the facility at any time."

More recently, under Article L.593-18 of the French Environment Code, it is specified that "the operator of a basic nuclear installation must perform regular safety reviews of the facility while taking into account best international practices. The purpose of a periodic review is to assess the extent to which the facility complies with applicable rules and to reassess any risks and drawbacks that the facility presents with regard to the interests mentioned in Article L.593-1, taking into account the state of the facility, operating experience, advances in knowledge and rules that apply to similar facilities. These reviews must be held once every ten years. A different interval may, however, be specified under the terms of the authorization, if this is justified due to specific characteristics of the facility. In the case of facilities that come under Council Directive 2009/71/EURATOM of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear facilities, periodic reviews must be held at least once every ten years."

Periodic reviews provide the operator with an opportunity to carry out a detailed safety review at each facility and to search for ways to improve facility safety with a view to ensuring, as far as possible, similar, if not the same, levels of safety as those achieved for more recent facilities. Periodic reviews, carried out once every ten years, are therefore also closely linked to the safety improvement process that entails analysing feedback on routine operations at nuclear facilities.

It should also be noted that, in France, nuclear power reactors are also subject to thematic reassessments taking into account specific subjects such as technological advances driven by manufacturers (involving, for example, fuel), new knowledge on complex subjects developed under research and development programmes (such as core-melt accidents), or more generic subjects (for instance, assessing the radiological consequences of accidents). Any changes required as a result of these thematic reassessments are usually integrated into the work packages created to apply changes decided for the ten-yearly outages, which include, in particular, a large-scale inspection programme.

Since first being brought into service, the nuclear steam supply systems in pressurized water reactors in the French nuclear power plant fleet have been subject to specific regulations regarding pressure equipment. In particular, the French Order of 26 February 1974 required hydrotests to be carried out on the main primary system once every ten years. The frequency of tests on the reactor containment is given in the operational limits and conditions[833]. In general, a series of in-depth tests and inspections was provided for and continue to be carried out every ten years, including the following:

– a hydrotest on the main primary system (reactor vessel, pressurizer, main pipes, steam generators). Regulations relative to pressure equipment stipulate that every ten years the nuclear steam supply system must be subject to a full inspection and requalification, including a hydrotest. A hydrotest is a general resistance test. It involves increasing the pressure in the reactor coolant system (RCS) to at least 20% above its design pressure, i.e. 207 bars, increasing pressure gradually through three intermediate steps. Sections of the main primary system are visually inspected by ASN inspectors to check for any problems during the test (leaks, deformation, marks, etc.). A qualified acoustic emission monitoring process is used during the test to detect any release of mechanical stress, including in areas that cannot be accessed to perform visual inspections;

[833] See Chapter 20 on general operating rules.

- an inspection of the reactor vessel using robotic inspection equipment to check the state of welds and the stainless steel liner, and for any changing defects (such as vessel 'underclad defects' – see Section 27.2.1);
- an examination of steam generator tubes;
- a test on the reactor containment[834] to check its mechanical strength and leak rate, during which in-containment pressure is increased to its design pressure using about ten compressors.

These operations are performed during reactor shutdowns scheduled as part of the ten-yearly outage, which lasts for several months. A ten-yearly outage includes many other checks, tests and changes, some of which are defined during studies associated with the periodic review. This will be illustrated below in the section on the first ten-yearly outage carried out at the Fessenheim and Bugey nuclear power plants.

This discussion does not set out to describe all the periodic reviews ever carried out on the various reactors in the French nuclear power plant fleet. Instead, focus has been placed on the periodic review associated with the third ten-yearly outage of the 900 MWe series, given that these are the oldest reactors to which the entire review process – which has been improved over the years – has been applied. Other aspects covered involve the current review in progress, associated with the fourth ten-yearly outage, which incorporates the plans put forward by Électricité de France (EDF) to extend the operating lifetime of the reactors beyond the 40 years defined in the design basis of certain systems.

30.2. History of periodic reviews in France for nuclear power reactors[835]

30.2.1. Reactors other than PWRs in the French nuclear power plant fleet

In France, gas-cooled reactors, or GCRs (cooled by carbon dioxide gas, using graphite as the moderator and natural uranium in metal form as fuel), the first French pressurized water reactor at Chooz (Ardennes), known as Chooz Unit A, a 245 MWe reactor, and then the PHENIX SFR reactor (a 563 MWth/250 MWe sodium-cooled fast-neutron reactor) underwent safety reviews after they had been in operation for between ten and fifteen years. In the following discussion, the term 'safety review' will

[834] For more information regarding reactor containment inspections and tests, readers may refer to Section 6.2.4 in Nuclear Power Reactor Core Melt Accidents – Current State of Knowledge, D. Jacquemain et al., Science and Technology Series, IRSN/EDP Sciences,2013.

[835] Some examples of major periodic reviews carried out for research reactors in France can be found in IRSN's work on safety in research reactors: Elements of Nuclear Safety – Research Reactors, J. Couturier et al., Science and Technology Series, IRSN/EDP Sciences, 2019.

be used, although at the time they were carried out, they were variously called reviews, complementary safety assessments or safety reassessments, depending on the case.

These safety reviews were held out of a concern to assess the safety of these reactors after they had been in operation for more than ten years or so, usually not in relation to any specific safety issue that may have arisen during their operating lifetime. In fact, assessments specifically examining safety at these reactors had previously been held on various occasions, following incidents or as part of a general drive to take operating experience feedback into account, but these did not assess overall facility safety, as is now the case with periodic reviews.

The first safety reviews of GCR reactors were held for the Chinon units A2 and A3 following a request from the Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN) to completely revise the safety reports for these reactors and to draw up general operating rules and on-site emergency plans. They were held in several stages up until 1988, when the last safety review of Bugey Unit 1 was conducted. These safety reviews helped identify the extent to which the safety requirements applicable to more recently designed or built reactors (especially pressurized water reactors) could be taken into account on older reactors and also to identify any measures that could introduce improvements. Any changes implemented generally allowed these reactors to continue operating under conditions considered to be acceptable at that time[836].

A safety review was conducted on the first pressurized water reactor built in France (Chooz Unit A) starting in 1983, primarily in light of the design adopted for the 900 MWe reactor series. The operating conditions of frequently used systems were assessed, taking into account any anomalies and incidents that had occurred, as well as any changes that had been made since Chooz Unit A was commissioned. Engineered safety systems were subject to systematic analysis based on the design criteria applied to 900 MWe reactors. Similarly, general operating rules were assessed with a view to bringing them into line with the general operating rules applicable to 900 MWe reactors, taking into account the specific characteristics of Chooz Unit A. Thus, in addition to improving documentation related to the safety analysis report and the operational limits and conditions, some major changes were made, such as installing a new steam generator emergency feedwater system, a remote shutdown station[837], and new post-accident instrumentation, as well as improving automatic startup of the safety injection system in the reactor coolant system and the spray system in the containment building.

Last, the safety review of Chooz Unit A led to verification of the facility's ability to withstand earthquake conditions, given that earthquake risk had not been taken into

[836] Significant cracks were detected in the Chinon Unit A3 cooling system pipes, causing problems that eventually led to decommissioning of the reactor.

[837] The Remote Shutdown Station is an engineered safety system placed outside the control room, which, in the event that the control room is no longer operational, can be used by the operating crew to bring the reactor to a safe shutdown state (and is distinct from the safety-parameter display system in the control room).

account in the reactor design. The seismic response spectrum as per Regulatory Guide 1.60, set to 0.1 g, was adopted for carrying out the relevant checks, primarily for the reactor coolant system, the automatic reactor trip system, the residual heat removal system and the spent fuel pool.

Various safety reviews were carried out on the PHENIX power reactor, which had first gone critical in 1973 and was scheduled for decommissioning in March 2009.

The first safety review on this reactor was carried out in 1986 in what was referred to as a 'safety reassessment'. The Central Service for the Safety of Nuclear Installations had asked for a safety assessment of the reactor subsequent to damage sustained to certain systems when it first came into service (including the intermediate heat exchangers) and the documentation describing how this damage had been dealt with (safety report and supporting studies [on seismic hazards, industrial hazards, accident studies, including fuel melt in the reactor core, etc.], the general operating rules and the on-site emergency plan).

In 1989 and 1990 reactor trips occurred as a result of negative reactivity in the core which led the French Atomic Energy Commission (CEA) – the operator – to investigate the causes and, in particular, demonstrate that such reactor trips were not indicative of damage in the reactor core support structures. The extensive research relating to this, which entailed various studies and tests, including on the reactor itself, formed a sort of targeted safety reassessment, including a review of all the possible events that might initiate a rapid change in reactivity and the revision of certain accident studies. In 1993, on completion of these studies, the French Directorate for Nuclear Safety (*Direction de la sûreté des installations nucléaires*, DSIN) gave the go-ahead to restart the reactor, but with improved monitoring of in-core conditions and operation at reduced power (at 350 MWth, using two of the three secondary loops). The first phase in resuming operation involved completing the 49th cycle, which had been suspended due to the reactor trips caused by negative reactivity conditions. CEA wanted to continue operating this reactor for the equivalent of 720 days at full power. To be able to do this, a full safety review was required. In-depth inspection of the sodium lines and extensive renovation work on the reactor were launched and carried out in stages from 1994 to 2003. As part of this safety review, and since the reactor trips that occurred in 1989 and 1990 had still not been explained, the operator had to conduct a non-destructive test on the core support shell which is immersed in sodium (as per an innovative procedure developed by the operator), to ensure that it had not sustained any damage liable to affect its mechanical strength under the different potential stresses (especially seismic stress).

30.2.2. PWRs in the French nuclear power plant fleet (900 MWe, 1300 MWe and 1450 MWe)

In 1987, ten years after the Fessenheim Unit 1 reached criticality, a safety reassessment of the Fessenheim units 1 and 2 and the Bugey units 2 to 5 (all of which are CP0 series reactors) was launched at the request of the SCSIN. This aimed to:

- check that the safety analysis report remained consistent with the reactor's 'as-built' condition,
- ensure that advances in knowledge, including lessons learned from operating experience, were taken into account,
- identify any significant differences between the design of the reactors reviewed and the safety options adopted in more recent reactor design,
- assess the benefits to be gained in terms of safety by making changes to the facility or procedures.

While these aspects may seem obvious, they nonetheless emphasize how difficult it can be to decide exactly which subjects should be covered in the reassessment, in order to avoid a complete revision of the safety analysis (which would require resources incommensurate with the expected results) while ensuring that no major issues have been omitted. Other questions arose regarding the choice of references to be taken into consideration for the reassessment, the methods used to assess overall plant safety, or complementarity between the reassessment itself and the continuous process of monitoring facility operation and analysing safety, mainly through operating experience feedback. While this did not, in theory, involve making major modifications to the facilities' civil works or systems, the aim was to identify any changes or corrective measures that might significantly improve safety.

Last, for this first safety reassessment on the first group of CP0 reactors, Unit B4 at the Chinon nuclear power plant – representative of the plant series 'end state' for 900 MWe (CP2) reactors – and the texts applicable to the 1300 MWe and 1450 MWe reactor series were adopted as references.

The reassessment, completed in 1993, was conducted during the first ten-yearly outage of these reactors (from 1989 to 1992); it covered 12 different areas, divided into 53 subjects, including the following:

- internal and external hazards,
- engineered safety systems (design and operating experience feedback),
- the reactor coolant system, secondary system and auxiliary systems,
- confinement,
- the instrumentation and control system,
- operating the safety injection system (SIS) and containment spray system (CSS) based on the use of water recirculated from the sumps at the bottom of the reactor building,
- the absence of an intermediate cooling system for the engineered safety systems in reactors at the Fessenheim nuclear power plant,
- the thickness of the basemat of these reactors, and their behaviour in the event of a core-melt accident,

- equipment safety classification,
- accident studies,
- tests to be performed during the ten-yearly outage.

Reassessment of some of these 53 subjects took advantage of results from the very first ten-yearly inspection programme which had, at the time, already been carried out (in 1989) for Fessenheim Unit 1 (see Figure 30.1), which included[838]:

- performing a hydrotest on the main primary system,
- inspecting the reactor vessel using the in-service inspection equipment, including, in particular, inspecting the reactor vessel inner wall to a depth of 30 mm (see Section 27.2), near the two weld seams in the most highly irradiated zone of the reactor vessel,
- searching for any vessel underclad defects caused by generic cracking, discovered in 1979 on reactor vessel nozzles in 900 MWe reactors,
- inspecting the tubes that cross the vessel lower head (associated with the in-core measurement instrumentation system), in light of the generic thinning phenomenon affecting these tubes[839] detected in 1985 in some reactors,
- measuring looseness in the core baffle and fasteners used on the lower reactor internals,
- a strength test and leak test on the reactor containment.

Tests were also scheduled by EDF during this first ten-yearly inspection programme of Fessenheim Unit 1. Nonetheless, following discussions with the safety organizations, other tests were carried out, including the following:

- tests on the SIS and CSS systems in sump water recovery mode and the borated water tank in the pool cooling system (the refuelling water storage tanks, RWST),
- a test to requalify the essential service water system (ESWS) under worst-case scenario conditions (lowest possible water level in the Grand Canal of Alsace),
- a pressure relief test on the SEBIM™ steam bleed valves of the pressurizer at low pressure in the feed and bleed mode, as required in certain accident situations,
- a test to qualify the containment filtered venting system and the associated U5 operating procedure (see Chapter 17), taking advantage of the test configuration set up for the containment hydrotest.

[838] See Chapter 27 on in-service monitoring and inspection of equipment, in which some of the subjects and inspections mentioned here are presented and discussed in greater detail.

[839] A phenomenon also known as 'thimble tube wear'.

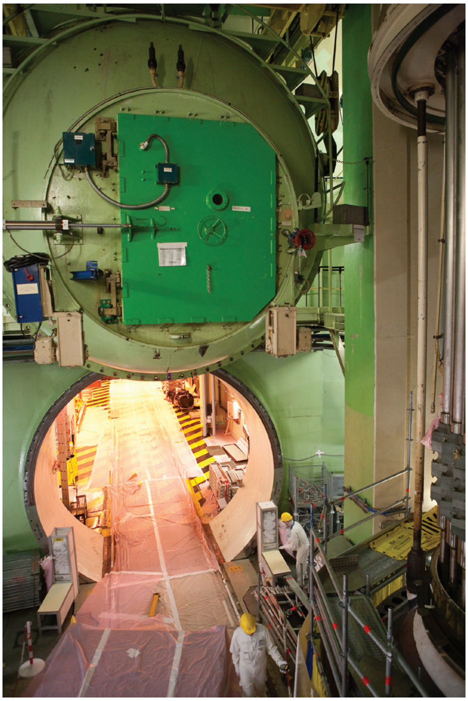


Figure 30.1. Opening the equipment hatch during a ten-yearly outage at the Fessenheim nuclear power plant. Noak/Le bar Floréal/IRSN Media Library.

The safety reassessment carried out on the Fessenheim and Bugey reactors led to many changes, mainly to the engineered safety systems, including:

- doubling the number of air circulator fans in the containment atmosphere monitoring system (ETY) to reduce any risk of hydrogen explosion inside the containment in an accident situation,
- replacing the filters in the SIS-CSS sumps to reduce any risk of clogging when these systems are operating in water recirculation mode,
- automating switching of the SIS and CSS systems to the water recirculation mode,
- installing a redundant suction line in the low-head safety injection (LHSI) system for intake from the RWST tank,
- replacing the heat exchangers in the CSS with new, more robust heat exchangers (made of titanium), bearing in mind that, in the Fessenheim reactors, cooling under accident conditions is ensured by direct intake from the natural environment (the Rhine River), without any intermediate system.

As of 1993, lessons were learned from this first safety reassessment of reactors in the French nuclear power reactor fleet. In general, this first experience confirmed the advantages of reassessing safety, as it also provided an opportunity, focusing on points considered as significant, to assess anomalies observed since startup and the corrective actions taken. It mainly confirmed the effectiveness of the safety improvement process, drawing on feedback, new knowledge and safety studies, such as the studies undertaken in the wake of the Three Mile Island accident (see chapters 32 and 33), studies on the 'complementary domain of events' (Chapter 13) and research on reducing the consequences of core-melt accidents, which included emergency response management (chapters 17 and 38). Nonetheless, this process was not designed to assess the adequacy of certain safety measures, particularly those systems that are not used under normal operating conditions or that are involved in preventing risks associated with certain internal or external hazards that occur rarely or are unlikely to occur. Advances in knowledge did not necessarily translate into actual improvements in safety at facilities, but rather to improvements in safety assessment.

This is why a new procedure for reviewing safety, initially proposed by IPSN and formalized in cooperation with EDF and the DSIN, was adopted. This review aims to cover two key aspects:

– first, the **Compliance Review**, to check that the facility complies with the applicable safety baseline[840] (including, in particular, compliance with the facility description and the safety demonstration support documents presented in the safety analysis report),

– and second, the **Safety Reassessment**, to take into account new information (new-build design, operating experience feedback, studies and research, knowledge, requirements and standards, etc.) that may have been developed since the preceding safety review.

This process, and the concepts related to it, are described further on.

Over time, improvements were made to the safety review process, based on feedback and lessons learned from reviews conducted previously.

30.3. Periodic review process for PWRs in the French nuclear power plant fleet

30.3.1. Regulations

Up until the adoption of the French law of 13 June 2006 on Nuclear Transparency and Security (Act 2006-686 of 13 June 2006, known as the TSN Act), safety reviews relative to basic nuclear installations were held in accordance with Decree 63-1228 of 11 December 1963 (amended in 1973, 1985, 1990 and 1993), in application of

[840] One other (initial) aspect had been defined for the first reviews held in application of this procedure, namely the definition of exactly what is covered in the 'safety baseline'.

Article 5 thereof (see the section on periodic reviews cited in the introduction to this chapter*)*.

This law, which was not officially cited in relation to pressurized water reactors, did not make it a systematic requirement for facility operators to conduct safety reviews at their facilities, nor did it set out any specific requirements regarding the frequency of reviews. EDF therefore began to conduct safety reviews on pressurized water reactors at the request of and in cooperation with the French safety authority.

The TSN Act, enacted in the French Environment Code, made safety reviews for basic nuclear installations mandatory, required that they be conducted periodically, and defined the objectives and procedures applicable to their implementation. The objectives and procedures of periodic reviews are set out in the following articles under Book V, Title IX of the French Environment Code, under the heading *La sécurité nucléaire et les installations nucléaires de base* (Nuclear Security and Basic Nuclear Installations):

- Article L.593-18 cited above in the introduction to this chapter.
- Article L.593-19: "The operator shall submit to the French Nuclear Safety Authority (ASN) and the minister in charge of nuclear safety a report describing the conclusions of the review required in accordance with Article L.593-18 and, where applicable, the measures it proposes to take in order to remedy any anomalies identified or to improve the safety of the installation. After analysing this report, ASN may impose new technical requirements. ASN shall submit its analysis of this report to the minister in charge of nuclear safety."

Thus, under the terms of Article L.593-19 of the French Environment Code, the requirement to carry out a periodic review is considered to have been met when the operator submits the review report to ASN and the minister in charge of nuclear safety. The date on which this report is submitted is the start date for the next ten-year period within which the operator is required to submit its next report.

A decision relative to periodic reviews of basic nuclear installations is currently being prepared by ASN[841] (supported by IRSN), aiming to specify the objectives and the scope of a periodic review, together with the procedures for conducting the review. In particular, this will specify the subjects that must be addressed in the Periodic Review Strategic Plan (*Dossier d'orientation du réexamen*, DOR – see Section 30.3.2) and the Periodic Review Final Report (*Rapport de conclusions du réexamen de sûreté*, RCRS).

For its part, EDF has undertaken to carry out periodic reviews on its reactors during the ten-yearly outages[842]. As highlighted in Section 30.1 above, many of the inspections and tests that must be conducted every ten years are performed within the framework of these ten-yearly outages, thereby enabling the operator to present

[841] The draft decision can be consulted on the ASN website.

[842] In French, the abbreviation 'VDn' may be found in the documentation, referring to the nth ten-yearly inspection programme, or *Visite Décennale*. The abbreviation VD3 900 thus refers to the third round of ten-yearly inspections of 900 MWe series reactors.

an up-to-date inventory of its plants in the periodic review final reports. Furthermore, ten-yearly outages last for a significant period of time, thereby providing an opportunity to implement any engineering changes that may be required as a result of the periodic review studies, and to prepare new operational documents. In addition, EDF organizes work packages to apply any changes (to documentation and equipment systems), thus making it easier to ensure consistency between facilities and operational documentation.

30.3.2. Outline of a PWR periodic review

▶ The 'plant series' approach

The concept of 'plant series' is not mentioned in the French Environment Code, which refers to periodic reviews of basic nuclear installations. However, the reactors in the French power plant fleet are designed, built and operated within the framework of a given technology series (900 MWe, 1300 MWe and 1450 MWe reactor series), and are grouped together at sites (with two, four or even six units built at the same site). Current practice regarding pressurized water reactors thus entails carrying out periodic reviews according to two key phases:

- a generic phase, during which studies related to the plant series in question are carried out, covering technical aspects common to the reactor units in that series (including engineered safety systems, accident studies, study methods, complementary domain of events, etc.). The conclusions drawn from these studies (changes in requirements or the safety demonstration, engineering changes, etc.) are applied to each reactor unit in the series when the periodic review for that unit is conducted;
- the actual reactor unit review phase, which covers site-related aspects (including external hazards) or the specific characteristics of the unit in question (state of civil works structures and specific components, systems, etc.).

This practice implies that the operator must carry out generic studies on a plant series well in advance of the first ten-yearly outage to be conducted on a reactor unit in that series, given the extent of the studies to be conducted (and the time required by the safety organizations to review them), and keeping in mind the fact that the last reactor unit in the series (usually the most recently built unit) will not benefit from the updated safety baseline and any related improvements until a much later time. For example, there are thirty-four 900 MWe reactors in France, commissioned over a period of ten years, from 1977 to 1987. The ten-yearly outage, which determines the date of the periodic review, for all the units in a series, will therefore be scheduled accordingly, over a period of about ten years. In other words, the most recently built unit in a series will be reviewed ten years after the review of the first unit in the series. An illustration of the schedule for generic studies conducted for the different plant series is shown in Table 30.1 at the end of this chapter.

▶ Purpose and content of periodic reviews

Before describing the purpose and content of periodic reviews, it may be useful to recall what is meant by the notion 'safety baseline', introduced very briefly in Chapter 2.

In the early 1990s, especially when the first periodic reviews were conducted according to the two phases mentioned above, the safety baseline for a nuclear power reactor, was (conventionally) made up of:

- the applicable regulatory texts (laws, decrees, orders and circulars),
- the applicable fundamental safety rules,
- the Safety Analysis Report and the General Operating Rules,
- the design and construction rules relative to pressurized water reactors (RCC-P for PWR system design, RCC-C for fuel, RCC-M for mechanical components, RCC-G for civil works, RCC-E for electrical components) – texts prepared by industrial manufacturers, which may have been, or are, subject to approval or comments by the French safety authority (see Section 2.5-b),
- any additional documents used to support the Safety Analysis Report.

As mentioned in Chapter 2, certain documents also submitted to ASN when applying for construction and operating authorizations, including the on-site emergency plan and the impact study, must also be added to the list above.

To summarize, the safety baseline can currently be divided into three groups of documents:

- documents such as regulatory and quasi-regulatory texts, ministerial decisions and requirements set out by ASN which apply to the facility, together with the safety objectives, national and international standards applied by the operator, design codes and standards and other reference texts used. Together, these documents form the 'requirements' part of the safety baseline, even though this may include documents that do not all cover the same scope, for example, the 'defined requirements' associated with items important to protection in a facility, based on studies presented in the safety analysis report or consistent with such studies;
- the methods, rules and criteria used to prepare studies on various operating conditions (including the complementary domain of events) and hazards in the safety demonstration; these methods, rules and criteria may, in the case of certain operating conditions or hazards, be grouped together in specific 'study baselines' (such as the LOCA baseline, severe accidents baseline, and extreme cold weather baseline, to name a few);
- documents relevant to facility operation: the general operating rules (including the operational limits and conditions and operating rules – which form part of the 'operating baseline'), and the on-site emergency plan.

To achieve the objectives set out in Article L.593-18 of the French Environment Code, periodic reviews of pressurized water reactors in the French nuclear power plant fleet are divided into two parts, as mentioned above:

- A **Compliance Review**, based not only on inspections but also on studies; this review primarily aims to check that[843]:

    - the design of reactors in the plant series complies with applicable requirements, and that the safety demonstration, covered in the safety analysis report, is still valid (compliance studies);

    - the actual state of each reactor unit complies with the required state, including any changes made to the initial design that may have been authorized), including by means of in situ inspections (compliance checks); these checks include:

        - a plant unit compliance review; it aim at checking that structures (civil works structures and metal structures), and selected systems and components comply with the applicable safety baseline prior to the safety reassessment described further on;

        - a complementary investigation programme[844], consisting of taking samples to check that the assumed absence of deterioration in certain systems and structures can be confirmed, particularly in the case of systems and structures that are not covered by periodic inspection programmes (where no degradation mode has been identified).

    These checks are mainly designed to ensure that all ageing-related degradation phenomena are recognized and monitored.

    To summarize, the aim of the compliance review is thus to check that the requirements on which the current operating authorization is based are still being met. It may identify shortfalls or degradation at the facility that will require further study or changes to the facility or its operating procedures. The best inspection practices available must be applied as far as possible.

- A **Safety Reassessment**, which takes into account any new facts that have arisen or developed since the preceding safety review. For example:

    - the safety objectives applied to the more recent reactor units;

    - changes in applicable regulations and quasi-statutory regulations, as well as in codes, standards, etc.;

    - operating experience feedback from reactor units in service or other facilities;

[843] For example, compliance of the chemical and radiological conditions at the site and in the environment must also be reviewed. These aspects are not dealt with in the rest of this chapter.

[844] A complementary investigation programme is established for each plant series.

- changes in practices, including those from other countries;
- changes in the technological and scientific data and knowledge relative to the various component parts of the facility (fuel, metal structures [heavy components, etc.], civil works, equipment and items such as pumps, different types of valve, diesel generators, etc.) and the surrounding environment (population, transport routes, industrial activities, intensity of hazards, etc.); such changes may be the result of research and development carried out at national or international level;
- changes relating to human, social and organizational factors (management, workforce skills, human resource management, human-machine interfaces, policy on safety and competitiveness, etc.).

ASN's draft decision mentioned above also requires (see Article 2.3.4) a reassessment of safety margins for extreme situations, in order to ensure that there are no 'cliff-edge' effects[845] – this reassessment is recommended in Article 3.4.1.2 of ASN Guide No. 22.

To begin the safety reassessment, the operator prepares a new requirements baseline, submitted to the safety organizations for review. It may be necessary to revise the studies that support the safety analysis report with regard to operating conditions and internal and external hazards in order to confirm that the defined requirements and criteria have been met. It may also be necessary to update the requirements and criteria. These studies are often collectively referred to as reassessment studies.

The aim of a reactor safety reassessment is therefore to improve reactor safety as far as reasonably possible, beyond the level achieved when the reactor was initially designed and built, and beyond the improvements attained through any subsequent changes.

Upon completion of these studies, the operator is ready to establish the new safety baseline for the facility, as described above.

Furthermore, the two parts of the periodic review lead to the definition of two sets of changes:

– changes designed to correct any deviations found with regard to the applicable safety baseline,

– and changes resulting from the safety reassessment itself, often grouped together in what is referred to as the 'ten-yearly outage change package'[846].

[845] In this draft decision, it is stipulated that, where a cliff-edge effect is detected, the operator must report on "the impact this may have on the nuclear safety demonstration and, where appropriate, the need, regarding defence in depth, to develop new items important to protection, to change the existing items important to protection or to change the requirements defined for the items important to protection present at the facility or placed under the responsibility of the operator."

[846] In some cases, these changes may be divided into several work packages.

▶ The Periodic Review Strategic Plan

Before conducting a periodic review of a facility, the operator prepares a Periodic Review Strategic Plan, which must then be submitted to ASN[847].

This strategic plan sets out the objectives of the review, prioritizes the themes approached, and specifies the defined baselines (those currently applicable and any new baselines proposed).

It describes and supports the outline, approach and methods that the operator intends to implement in conducting the compliance review of the items important to protection within the facility, including the in situ inspection programme.

The periodic review strategic plan must highlight any major changes planned to the facility and its operating conditions (fuel management, power increase, etc.), and in the facility environment (especially any changes to transport routes near the site, the transportation of hazardous materials, the industrial environment or the local population).

For each theme covered in the safety reassessment, the strategic plan must include the related objectives, the assumptions taken into consideration, and the methods and rules to be used for studies (study baselines).

Lastly, the sections of any documents submitted as part of the application for the facility construction authorization or the operating authorization which the operator intends to significantly revise upon completion of the periodic review, must be identified.

After analysing the periodic review strategic plan, ASN will either approve it, possibly subject to certain changes or submittal of additional information, or reject it.

▶ The Periodic Review Final Report

After completing all inspections and studies, for each reactor unit, the operator must submit to ASN and to the French minister in charge of nuclear safety, a report on the conclusions of the periodic review (a document required under Article L.593-19 of the French Environment Code), reporting on both parts of the periodic review.

The summary report on the compliance review recalls the applicable requirements, the approach and methods implemented, including the in situ inspection programmes, and the results of the review, identifying any deviations and the measures taken to correct them, along with support data.

The periodic review final report must also present the results of periodic tests and requalification procedures performed on the confinement barriers (reactor containment, main primary system, etc.).

[847] The periodic review strategic plan may be entirely or partly generic, covering several plants; for example, for the French nuclear power plant fleet, it may cover all reactor units belonging to the same plant series.

The safety reassessment summary report is accompanied by a presentation of any changes to the facility or operating procedures, either implemented or planned, along with support data, and a presentation of any interim measures that may have been decided pending implementation of the abovementioned changes; a schedule for performing the decided changes is included with this report. The conclusions of the periodic review final report substantiate the ability of the facility to continue operations under satisfactory safety conditions.

After analysing the periodic review final report, ASN may impose new technical requirements as a condition to continued operation of the unit in question. ASN also submits its analysis of this report and any requirements imposed to the minister in charge of nuclear safety.

30.4. Case of the review associated with the third ten-yearly outage of 900 MWe reactors

The process applicable to periodic reviews has been refined in the course of the successive reviews conducted on the various reactor series. The review associated with the third ten-yearly outage (VD3) of the 900 MWe series can be used to illustrate this process in detail; the review corresponding to the fourth ten-yearly outage (VD4) will be discussed in Section 30.5. The case of the periodic review associated with the VD3 900 outage is especially interesting in that, since these are the earliest reactors in the French nuclear power plant fleet, which are due to reach the end of their design-basis operating lifetime within the ten years following VD3 900, the aspects related to system ageing were examined earlier than planned and in particularly close detail. In addition, the review associated with the VD3 900 outage provided an opportunity to implement a specific safety requirements baseline designed to mitigate core-melt accident situations – which had not been considered in the initial design of the French nuclear power reactors then in service, but were taken into account in the EPR design. These considerations had nonetheless led to improvements applied to the French nuclear power plant fleet in the measures taken following the Three Mile Island accident.

The example of the VD3 900 outage should not eclipse the major changes implemented as a result of the earlier periodic reviews on 900 MWe reactors, including the following:

- the water tanks in the steam generator emergency feedwater system (EFWS) and the RWST tanks were upgraded to comply with earthquake resistance requirements (this deviation affected all the 900 MWe reactors),
- a measure had been implemented to mitigate the possibility of a common-cause failure on the 6.6 kV AC emergency-supplied distribution systems (LHA and LHB) (as a result of feedback on an event that occurred in 1990 at the Cruas-Meysse nuclear power plant),

– a change was made to enable (radioactive) effluent collected in the sumps in the nuclear auxiliary buildings to be pumped back into the reactor building (a post-TMI measure).

Generic studies for the periodic review associated with the VD3 900 outage were launched in 2002 and completed at the end of 2008. The first 900 MWe reactor to undergo a third ten-yearly inspection was Tricastin Unit 1, in 2009. Figure 30.2 shows the key stages in this periodic review.

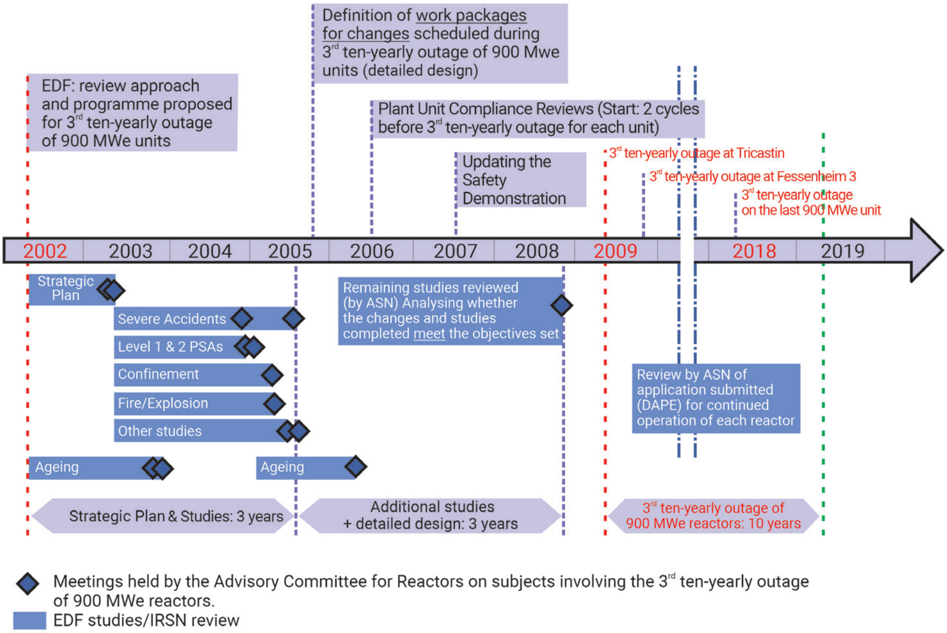

Definition of work packages for changes scheduled during 3rd ten-yearly outage of 900 Mwe units (detailed design)
EDF: review approach and programme proposed for 3rd ten-yearly outage of 900 MWe units
Plant Unit Compliance Reviews (Start: 2 cycles before 3rd ten-yearly outage for each unit)
Updating the Safety Demonstration
3rd ten-yearly outage at Tricastin
3rd ten-yearly outage at Fessenheim 3
3rd ten-yearly outage on the last 900 MWe unit
2002
2003
2004
2005
2006
2007
2008
2009
2018
2019
Strategic Plan
Severe Accidents
Level 1 & 2 PSAs
Confinement
Fire/Explosion
Other studies
Ageing
Ageing
Remaining studies reviewed (by ASN) Analysing whether the changes and studies completed meet the objectives set
Review by ASN of application submitted (DAPE) for continued operation of each reactor
Strategic Plan & Studies: 3 years
Additional studies + detailed design: 3 years
3rd ten-yearly outage of 900 MWe reactors: 10 years
Meetings held by the Advisory Committee for Reactors on subjects involving the 3rd ten-yearly outage of 900 MWe reactors.
EDF studies/IRSN review

Figure 30.2. Key stages in the periodic review associated with the third ten-yearly outage of 900 MWe units (VD3 900). IRSN.

The work programme proposed by EDF in 2002 was assessed by IRSN, focusing on the following subjects:

– the possibilities for improving 900 MWe reactors to meet the general safety objectives used in designing the EPR. Nonetheless, given the differences between 900 MWe reactor design and the EPR design, this analysis took a pragmatic approach and assessed, for each of these safety objectives, whether the improvement was technically feasible and if it significantly improved safety;

– the conclusions resulting from earlier periodic reviews (such as the reviews associated with the VD2 1300 outage), the studies undertaken in other contexts regarding safety issues, and national and international operating experience feedback.

In 2003, following this assessment, the main subjects defined for the generic reassessment studies were as follows:

- checking the design of civil works and systems,
- control of ageing in civil works structures and equipment,
- accident scenarios, including scenarios with core melt, assessing the risks of core melt and release to the environment (Level 1 and 2 Probabilistic Safety Assessments [PSAs]) and containment behaviour,
- internal hazards,
- external hazards of natural origin or that may be caused by human activities.

About thirty subjects in all were approved, which were then to be used to specify about sixty generic equipment changes, plus some changes specific to certain sites related to addressing external hazards, for example. The main checks and studies conducted are described below, indicating some of the changes adopted as a result of the studies.

Several baselines defined by EDF were used in the context of the VD3 900 outage, including those related to: criticality of fuel stored in the reactor pool in the reactor building and in the spent fuel pool in the fuel building; assessing the radiological consequences of accidents without core melt; accidents with core melt; the 'new complementary domain' events[848]; the safe lowest water table level (loss of heat sink due to low water levels) and the pumping station; the risk of internal explosion at a site, etc.

30.4.1. Plant unit compliance reviews, the complementary investigation and ageing management

30.4.1.1. Plant unit compliance reviews

Plant unit compliance reviews performed in situ for 900 MWe reactors in the context of the VD3 900 outage covered topics including the following:

- civil works: an assessment of the implementation of the maintenance programmes applicable to civil works important to safety was conducted, together with inspections of buildings and structures that had not been inspected during the previous compliance review;
- equipment anchoring systems: compliance with construction drawings and adequacy of maintenance carried out on systems used to anchor any equipment required to allow reactors to reach and maintain a safe state in the event of a seismic margin earthquake were checked;

[848] See Section 13.4.

- implementation of the ‘event-level’ earthquake approach (see Section 12.3): compliance of any changes specifically designed and implemented for each reactor was checked;
- support systems for electrical cable trays: cable trays carrying significantly high loads were checked for their resistance to seismic margin earthquake conditions; systems were checked for installation faults and load-bearing capacity;
- functional capability of equipment used in incident and accident operating procedures: each site was checked to ensure organizational procedures were implemented to guarantee the functional capability of this equipment; availability of all mobile equipment required for this purpose was checked, as well as the relevant assembly work procedures;
- confinement and ventilation: integrity of room leaktightness was checked (penetrations, doors, floor drains, etc.) and ventilation ducts important to safety were inspected;
- criticality risk prevention: the existence of equipment, systems and administrative measures required to prevent criticality risk was checked, as well as compliance of the implemented measures with the relevant specifications;
- external flooding: improvements made as the result of feedback from the partial flooding of the Blayais NPP site in December 1999 were checked to ensure they were compliant with applicable specifications;
- fire protection systems: an analysis was conducted to determine which measures, if any, remained to be implemented as part of the firefighting action plan (see Section 11.6).

For some of the subjects and functions that were inspected, no deviations were found. However, several hundred nonconformities were identified, although with little significant or immediate impact on safety (many were related to a large number of items such as civil works, equipment anchoring systems, cable trays, etc.).

30.4.1.2. Complementary investigation programme

The complementary investigation programme (CIP) for 900 MWe reactors implemented during the VD3 inspections was designed to examine, by means of sampling, the passive components (pipes, tanks, etc.) that were not inspected as part of maintenance programmes, regulatory inspections (pressure equipment) or specific inspections required subsequent to the identification of generic or specific deviations or issues. The investigations carried out, based on a defence-in-depth approach, focused on areas that were not considered to be sensitive in the design studies, in order to check for any phenomena that had not been considered or dealt with up until then and, more generally, to check that existing maintenance and monitoring measures were adequate for ensuring facility operation under satisfactory safety conditions.

The tests and inspections scheduled in the CIP conducted during the VD3 900 outage supplemented those carried out during VD2 inspections on passive components of the main primary system and the main secondary system, together with pipes, tanks and heat exchangers that are not part of either of these main systems.

In addition, as part of ageing management, EDF was asked to define and conduct inspections focused on reactor containments and civil works. Regarding structures and equipment that may prove sensitive to ageing in the areas of electrical equipment, valves, rotating machines, lifting equipment, fire safety equipment and automatic control systems, the inspections set out by EDF, under either the CIP (civil works, main primary system, etc.), or any other programme, were found to be adequate by the safety organizations.

The results of all the inspections performed under the CIP allowed EDF to complete the fitness-for-service file to be submitted (*Dossier d’aptitude à la poursuite de l’exploitation*, DAPE) for approval of continued operation of the reactors.

30.4.1.3. Ageing management

At the beginning of the 2000s, EDF proposed a general approach for managing ageing at its plants, consisting in identifying the structures, systems and components (SSCs) important to safety affected by ageing processes that could, between 30 and 40 years of operation, result in the degradation of their performance or reliability and thus have an impact on the safety (and availability) of these plants. Out of about 15,000 SSCs, 500 pairs linking an SSC with an ageing process were identified; each pair was described in an ageing analysis sheet setting out the operating and maintenance measures required to manage it. Any SSC for which a ‘sensitive’ ageing analysis sheet has been drawn up (in other words, for which the potential consequences of ageing are considered significant in terms of safety, and for which there are no measures that will prevent or mitigate the consequences of ageing, or which cannot easily be monitored) is subject to a specific ageing management programme. Twelve generic SSCs have been identified, including the reactor vessel, the reactor containment and I&C systems.

EDF built on this approach to draw up the DAPE applications for continued operation of the aforementioned SSCs installed at each of the 900 MWe reactor units at the time of the VD3 900 outage, starting with Tricastin Unit 1.

30.4.2. Compliance studies on the design of civil works systems and structures

Studies were carried out on the design of certain structures, systems and components as part of the periodic review associated with the third ten-yearly outage of 900 MWe reactors, based on available feedback, the different functions assigned to these SSCs and the requirements relating to them within the framework of accident studies or according to the design options or rules. These studies formed a series of post-construction checks, similar to a ‘design review’.

▶ Verification of civil works design

Studies were conducted to check the validity of the design assumptions, criteria and methods used in the civil works design phase, and the systems associated with civil works, considered to be of primary importance to safety. These studies covered a large number of civil works, and have been used to assess the robustness of the design, construction and maintenance methods implemented with regard to civil works important to safety and, therefore, to check that they adequately fulfil the safety functions assigned to them.

▶ Enhancing reliability of the plant radiation monitoring system

Since 1994, the plant radiation monitoring system (PRMS), consisting of measurement instrumentation designed to check compliance with certain requirements related to safety, radiation protection and environmental protection, has undergone a series of improvements designed to make it more reliable. Nonetheless, also at the beginning of the 2000s, feedback on operation of the PRMS revealed a high rate of system failure.

Studies conducted within the framework of the periodic review associated with the VD3 900 outage, focusing on various aspects (operating feedback, consequences of ageing, preventing the risk of worker exposure to ionizing radiation, etc.) resulted in a number of changes being designed for this monitoring system, aimed, in particular, at resolving the identified reliability issues.

30.4.3. Studies to reassess system design

▶ Checking the functional capabilities of the safety injection system

The performance levels of the various water injection components that make up the safety injection system (SIS) are a key factor in the safety demonstration, especially under LOCA conditions. These components are used to cool the reactor core, allowing it to achieve and maintain a sub-critical state. New studies on loss-of-coolant accidents (LOCA) (see Section 30.4.5 below), changes in SIS design and operating procedures, and the detection, during periodic tests, of nonconformities affecting this system, led to a decision to reassess the functional capabilities of this system with regard to its different objectives within the context of the periodic review associated with the VD3 900 outage.

The following aspects were examined:

- determining the flow rates of water injected into the reactor coolant system as a function of the pressure in the reactor coolant system and the hydraulic characteristics of the pumps and various systems,
- assessing the extent to which the periodic tests performed were representative of all the possible configurations of the SIS under accident conditions and the relevance of the corresponding test criteria,
- identifying potential cliff-edge effects by studying the influence of SIS sensitivity to the characteristics of injection systems and their operation.

The results of these studies were used to confirm that the characteristics of the SIS are, overall, appropriate and do not need to be upgraded.

▶ Improving the reliability of water recirculation within the containment

As described in Chapter 9, in the event of any break in the reactor coolant system of a pressurized water reactor, reactor cooling is maintained by the safety injection system (SIS). The containment spray system (CSS) is simultaneously actuated to reduce pressure inside the reactor building. Once the tanks storing the borated water used by the SIS have been emptied, the SIS and the CSS systems continue to operate in a closed circuit, recirculating the water collected in the sumps at the bottom of the reactor building, after it has passed through filter screens. This configuration is designed to cool the fuel over long time periods.

It may be recalled (see Section 9.1.4) that partial clogging of the sump filters was found in 1992 during an event in a boiling-water reactor unit at the Barsebäck nuclear power plant in Sweden. In 1997, in relation to feedback on this event, IPSN launched a series of studies and research on possible clogging phenomena on the sump filters in pressurized water reactors in the French nuclear power plant fleet. The results led to a recommendation to conduct a specific review on the risk of clogging on the sump filters as part of the periodic review associated with the VD3 900 outage. In 2004, EDF therefore decided to change the design of these filters, with deployment of the new design completed in 2009.

Based on new knowledge, mainly developed by means of extensive experimentation carried out between 1999 and 2003, the periodic review performed in the context of the VD3 900 outage entailed the characterization of:

- the spectrum of debris likely to arrive upstream of the filters,
- the risks of clogging on the filter screen due to physical and chemical phenomena, liable to increase head-loss across the filters,
- the minimum head required in the sumps to ensure recirculation,
- any debris not blocked by the filters that could be carried into the SIS and CSS, and into the reactor.

These studies also incited EDF to modify some of the control valves with a low flow cross-section used on the safety injection system to prevent them from becoming clogged by any debris not filtered out by the sump screens.

As mentioned in Chapter 9, the complex[849] subject of the reliability of the cooling function in water recirculation mode ensured by the in-containment sumps is not yet closed.

[849] Research and development studies continue to focus on the risks of the sump filters becoming clogged and the consequences of this downstream of the filters. For more information, see, for example, Chapter 5 in Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2018.

▶ Reliability of the spent fuel pool cooling system

Studies carried out as part of the periodic review performed in the context of the VD3 900 outage focused on the measures implemented to manage certain events that could lead to the accidental draining of a pool used to store fuel assemblies, including spent fuel assemblies, bearing in mind that improvements to the measures designed to manage any risk of total loss of cooling of the water in this pool had already been adopted within the framework of the previous periodic reviews. More specifically, the objectives set out as part of the periodic review in the framework of the VD3 900 outage aimed to prevent certain scenarios likely to initiate inadvertent drainage and reinforce preventive measures by means of technical and organizational measures.

Possible radioactive release that could result from fuel assembly uncovery during handling operations in the fuel building were assessed. The probability of various initiating events liable to cause rapid drainage of the pool and the operating procedures planned by the facility operator should drainage of the pool begin were analysed. As a result of these studies, EDF deployed a series of changes designed to improve the management of certain scenarios involving drainage or uncovery of fuel assemblies during handling operations, including scenarios likely to result in rapid drainage or uncovery, including:

- automating shutdown of the pool cooling pumps and closure of the intake line if a very low water level is reached in the fuel building pool,
- improving the siphon breakers installed on the cooled water discharge line in the fuel building pool,
- creating redundancy of the static seals ensuring that the sluice gates in the reactor building pool are leaktight,
- changing to motor-driven closing of the isolation valve on the fuel transfer tube between the reactor building and the fuel building,
- installing more robust plugs on the reactor coolant nozzles (steam generator nozzle dams) so that they cannot be dislodged during reactor refuelling operations if an air-pressurized SIS accumulator is depressurized[850] while the transfer tube between the reactor building and the fuel building is open[851].

[850] The SIS accumulators are air-pressurized to drain them prior to core refuelling. However, they may be maintained under air pressure, or repressurized, when refuelling operations start, as was the case in the significant event that occurred on 7 September 2000 at Unit 5 of the Bugey nuclear power plant: an SIS accumulator had been repressurized in order to perform requalification tests on its water level sensors.

[851] In this reactor state, failure of a steam generator nozzle dam can cause large quantities of coolant to rapidly drain from the two pools, resulting in uncovery of the fuel assemblies during handling and a sustained loss of cooling in the fuel building pool.

30.4.4. Reassessment of reactor resistance to internal and external hazards

▶ Fire

The main studies for the safety reassessment performed in the framework of the VD3 900 outage focused on assessing the margins existing between a) the fire resistance of systems designed to protect the essential systems required to control the facility (i.e. those required to restore and maintain a safe state) and the fire resistance of systems used to provide protection against common-cause failure modes related to electrical wiring, and b) the likely duration of a fire in rooms where these protection systems are installed. The fire duration periods used[852] in designing these protection systems were calculated based on assumptions that were no longer valid, given the conditions that could impact the buildings containing pressurized water reactors in service. Given the uncertainty surrounding the fire resistance of these protective systems, EDF adopted a minimum required margin of ten minutes and made several improvements for cases where this margin was not met, including raising the fire resistance rating for certain systems and installing new firefighting measures.

The Level 1 probabilistic safety assessment on fire hazards developed by IRSN had demonstrated that the measures regarding equipment and procedures implemented by EDF as part of its firefighting action plan had significantly reduced the probable frequency of core melt due to fire. However, this study also revealed that certain rooms played a significant role in the overall residual frequency of core-melt events and recommended investigating what could be done to improve this situation. EDF set up a multi-point fire detection system in certain 48 V DC power supply cabinets located in the electrical rooms in question.

▶ Explosions caused by hazards inside facilities

Studies conducted by EDF regarding protection against the risk of explosion due to hazards inside facilities resulted in an exhaustive inventory of rooms presenting a risk of explosion in the event of a hydrogen leak and a series of additional measures to be taken to improve management of this risk.

A great many component and system changes were designed and implemented in these rooms, including the installation of hydrogen detection sensors, replacing components that were not explosion-proof with components designed for use in an explosive atmosphere, strengthening or protecting pipes carrying hydrogen and improving monitoring of these pipes, and replacing certain isolation valves on the pipes with high-integrity models.

[852] Based on what is known as the ‘DSN 144 curve’, now recognized as obsolete by EDF, IRSN and ASN.

▶ Internal flooding

In the framework of the VD3 900 outage, following partial flooding at the Blayais NPP site at the end of 1999, checks to confirm that the facility could withstand specific flooding scenarios had not yet been completed. Therefore, using the 'event-level earthquake' approach, the potential consequences of the simultaneous failure of all tanks not designed to withstand earthquake conditions installed in the nuclear auxiliary building were identified. These studies concluded that the existing outlets and retention systems would prevent any unavailability that could possibly occur in the event that the SSCs required to reach and maintain a safe shutdown state were flooded due to an earthquake.

▶ External hazards related to climate conditions

The various potential hazards related to climate conditions were covered in the initial design of 900 MWe reactor units, including characterization of the potential hazards and assessment of their possible consequences. For this reason, it was decided that in the context of the VD3 900 outage, a safety reassessment would be conducted on the ability of facilities to withstand hazards that had not, until then, been extensively studied in France, as well as hazards exhibiting characteristics that had changed since the time of initial facility design.

The studies conducted concluded that, given the locations of the various sites and their sensitivity to climate-related hazards:

- the risks associated with tornadoes and forest fires did not require any specific measures since the probability of tornadoes occurring was considered sufficiently low, and the impact of forest fires on facilities was considered to be limited;
- reassessment of hazards related to strong winds did not call into question the design of facility structures and civil works;
- risks related to frazil ice[853] and drifting oil slicks were managed by means of appropriate physical protection measures and warning systems; nonetheless, a more precise characterization of these risks and in-depth analysis of the related scenarios resulted in the decision to change the existing physical measures and operating procedures.

Last, following the heatwave of 2003, a programme was launched to verify the ability of sites to cope with risks related to heatwave events and drought. This work was to be actively pursued with the aim of implementing the necessary measures at all sites in the near future.

[853] As mentioned in Section 12.6, frazil ice is a specific phenomenon whereby a volume of water ices up when ice crystals that form in turbulent water agglomerate together and build up to such an extent that they block the turbulence, forming floating plates of ice. The conditions in which frazil ice develops occur when the water temperature falls below 0°C and the air temperature falls below -10°C.

▶ Reactor and site autonomy in the event of external hazards

The partial flooding of the Blayais NPP site in December 1999 highlighted how sensitive plants may be to common-mode external hazards, i.e. hazards that simultaneously affect all the units at a site. In addition to the lessons learned from this event with regard to the risks of flooding due to external causes (see Section 24.1), it seemed reasonable to extend this analysis to all external hazards (earthquakes, strong winds, extreme cold weather, etc.) and the possibility of them occurring simultaneously, bearing in mind the resulting potential for common-cause failure, with a view to verifying or upgrading the robustness of the facility design and operating procedures under such conditions. This led EDF to focus its attention on situations involving a total loss of the heat sink required for cooling the reactor units at a site (H1), and loss of power to the site's reactor units (H3, or station blackout).

The modifications decided as a result of the related studies entailed increasing fluid capacity (water, fuel oil and oil) at the sites and enhancing on-site power sources.

▶ Seismic reassessment

Continuing on from earlier reviews, seismic reassessment in the framework of the VD3 900 outage included a reassessment of the ground motion response spectra used to characterize the seismic margin earthquake (SME) for each site and analysis of the impact that this reassessment might have on the robustness of the reactor systems, by applying best practices and state-of-the-art technology in the field.

To ensure that structures, systems and components perform in a satisfactory manner in the event of an earthquake (in compliance with their functional requirements), it was decided to make certain changes, depending on the site, including strengthening of reinforced concrete structures, metal structures and equipment anchoring systems, as well as replacing some equipment items.

In addition, checks were carried out to confirm that safety-grade structures were not subject to any risks that could come from the turbine hall (which is not designed to withstand earthquake conditions).

30.4.5. Accident studies

Operating under accident conditions could have consequences that impact people and the environment, which explains why the safety reassessment conducted as part of a periodic review must include checking that the measures implemented to prevent and mitigate such consequences continue to meet the relevant requirements, while taking into account various changes that may have occurred, namely:

– changes affecting the design assumptions, methods and tools resulting from, among other things, advances in knowledge of certain physical phenomena, mainly through research,

– changes affecting operating conditions and practices,

– changes in safety approaches, which may require research on specific types of accident not covered in either the initial design studies or subsequent studies,

– changes to the facility that may affect the assumptions used in the initial design studies or subsequent studies.

▶ Risk of cold overpressure in the reactor coolant system

Previous assessments of the risk of cold overpressure in the reactor coolant system (RCS) in reactor shutdown states, conducted since 1997, revealed a need for improvements to prevent fast fracture in the reactor vessel, which could be caused by overpressure in the RCS at temperatures below 90°C. When the reactor is at power, the temperature in the RCS, about 300°C, is much higher than the ductile-to-brittle transition temperature of the ferritic steels used to build the vessel, which explains why there is no risk of fast fracture. However, neutron irradiation raises the ductile-to-brittle transition temperature of the steel used to make the core support shell and any sudden cooling of this steel due to a high-head injection of cold water via the safety injection system could cause a brittle fracture in the vessel.

In addition to improved operating procedures implemented previously, in the context of the periodic review associated with the VD3 900 outage, EDF decided to implement a change that entailed lowering the opening pressure of the safety valves on the pressurizer when the reactor coolant system is closed and the reactor is cooled using the residual heat removal system; this makes it possible to significantly reduce the likelihood of cold overpressure in the event of a loss-of-coolant situation requiring safety injection.

▶ Core-melt accidents

Following the accidents at the Three Mile Island and Chernobyl nuclear power plants, a vast range of studies were undertaken with a view to mitigating the consequences of a core-melt accident. Within the context of the safety review associated with the VD3 900 outage, EDF developed a baseline for core-melt scenarios (the 'severe accidents' baseline), setting out an approach, objectives and safety requirements relative to certain structures, systems and components. This focused on the following aspects in particular:

– the mechanical strength of the reactor containment during a core-melt accident, including in the event of a hydrogen explosion or core melt when pressure in the reactor coolant system is high,

– the resistance (the capacity to remain operational) of certain SSCs under the ambient conditions that may result from a core-melt accident, and particularly the ability to control the RCS depressurization safety valves in the event of a total loss of power (station blackout),

– the instrumentation systems that can be used to 'manage' a core-melt situation,

- the strategies to be implemented in the damaged reactor, including strategies for operating the in-containment spray system and the system used to inject water into the reactor pit[854].

The studies conducted led EDF to define a series of changes designed to significantly reduce the risk of containment failure and to ensure monitoring of the accident sequence, including:

- increasing the thickness of the basemat beneath the two units at the Fessenheim nuclear power plant (a subject previously studied during the first safety reassessment on these units),
- a change designed to make opening of the pressurizer safety valves more reliable in the event of station blackout (H3), to prevent high-pressure core melt,
- replacing some SSCs in the reactor building with SSCs qualified to withstand the conditions (pressure, temperature, etc.) liable to result from a core-melt accident,
- installing thermocouples in the reactor pit to detect any penetration of the reactor vessel by corium.

EDF also decided to install autocatalytic hydrogen recombiners inside the containment to prevent hydrogen explosion (see Section 17.5.4).

▶ Confinement

The aim here was to assess the confinement function provided by the 'third confinement barrier', not only under normal operating conditions (including outage) and design-basis accident situations, but also under core-melt conditions, primarily with reference to the baseline specified for the third ten-yearly outage in relation to this issue. As described in Chapter 6, the third confinement barrier is formed by the reactor containment (the reactor building), the penetrations in this containment (airlocks, sleeves, etc.), the boundaries on the secondary side of the steam generators, and ventilation and air filtration systems. Systems that may be required under accident conditions and in which radioactive substances may be transported out of the containment form an extension of the third confinement barrier.

The various measures designed to ensure the 'confinement' safety function were examined to establish the current state of measures taken in the facility, assess the performance of these measures and identify any possible improvements. This included examining, in particular:

- the mechanical behaviour and the leak rates of the different confinement barriers in 900 MWe reactor units. This analysis included a review of the results of general leak tests on these confinement barriers, the service life of each of

[854] See Chapter 17.

the systems used to monitor them, the main ‘pathologies’ to which they may be subject, and their resistance to design-basis and core-melt accident scenarios;

- the behaviour of the containment penetrations, including in the event of a core-melt accident, and including large openings such as personnel access airlocks and equipment hatches;
- management and distribution of leaks in the containment, which may either open directly into the environment, or into auxiliary buildings;
- the ‘extension’ of the third confinement barrier;
- the risk of coolant leaking directly out of the reactor containment;
- the leaktightness – provided by the actual building structures or by the ventilation systems – of auxiliary buildings into which radioactive fluids or gases might leak;
- radiological conditions in control rooms during a core-melt accident;
- the functional requirements and performance of the filtered venting systems for rooms within the nuclear island, other than the reactor building.

These studies demonstrated that there were no anomalies related to containment behaviour in the 900 MWe reactor units. Changes were, however, made to improve leaktightness on some of the airlocks and isolation valves. Last, it was found that additional investigations were needed to assess the concrete used in the containments and the coating on prestressing bars, before preparing applications for the continued operation (DAPE) of the reactor containments.

Regarding the airlocks used to access the reactor building, the study on the behaviour of the third confinement barrier under core-melt accident conditions led to improvements on the equipment hatch closure system to ensure its mechanical resistance to pressure spikes of up to 8 bars (see Section 14.3.3.2).

▶ Insights resulting from probabilistic safety assessments

With regard to Level 1 probabilistic safety assessments, the probabilistic objective set by EDF for the periodic review associated with the VD3 900 outage, namely a core damage frequency objective of less than 10^{-5} per reactor per year relative to internal events (at the time of the VD2 900 outage, the estimated value was 5×10^{-5}), was intended to help improve risk reduction by taking into account improvements already made to facilities.

The periodic review associated with the VD3 900 outage also provided an opportunity to conduct a Level 2 probabilistic safety assessment.

EDF learned a great deal as a result of the PSAs, leading it to implement certain measures to reduce core-damage frequency or reduce related potential release into the environment. Two measures are of interest here:

- the first aimed to reduce the risk of core damage involving containment bypass in the event of failure of a (CCWS) thermal barrier cooling coil in a reactor coolant pump (RCP). EDF applied changes to make isolation of the RCP thermal barrier more reliable by adding, on the CCWS system downstream[855] of the thermal barrier, a motor-driven pneumatic valve and a temperature sensor designed to trigger closure of the valve if the CCWS water temperature exceeded 100°C;
- the second aimed to improve the equipment hatch, as mentioned above.

The lessons learned from the PSAs carried out as part of periodic reviews in general, and especially the review associated with the VD3 900 outage, are described in detail in Section 14.3.

▶ Passive failure of an engineered safety system

Regarding the French nuclear power plant fleet, the rules applicable to studies on design-basis (reference) accident operating conditions stipulate that it is necessary to consider the case of a passive failure (i.e. affecting a static component, such as a pipe) of the safety systems after they have been in operation for 24 h; this failure is assumed to lead to a leak at a rate of 200 L/min that takes 30 min to isolate. Assessing the consequences of a more severe failure on the performance of the safety systems and on the environment – as applied in the EPR design[856] – confirmed that taking into account this more penalizing scenario did not affect the availability of the systems required to manage the abovementioned accident scenarios and does not lead to increased release to the environment

▶ Steam generator tube rupture

As part of the periodic review associated with the VD3 900 outage, changes were made to improve prevention of water overflow caused by a steam generator tube rupture (SGTR). These changes involved:

- first, the operating conditions of the steam generator emergency feedwater system (EFWS), improved by incorporating automatic shutdown of the steam generator main feedwater system (MFWS) and automatic isolation of the EFWS,
- second, operating procedures, improved by providing automatic cooling of the reactor coolant system by using the atmospheric steam dump valve MSBa of the undamaged steam generators to offset, as quickly as possible, the leak from the RCS by rebalancing the pressure between the damaged steam generator and the RCS.

Although these changes do not completely rule out the risk of water release, they do provide more time for the operators to implement procedures designed to prevent this release.

[855] A check valve is installed upstream of the thermal barrier.

[856] As part of sensitivity studies (see Section 8.4.2). This included leaks arising within 24 h or at a rate higher than 200 L/h (see ASN's Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors).

▶ Functional capabilities of equipment designed to manage ‘complementary domain’ event scenarios

The studies carried out as part of the periodic review associated with the VD3 900 outage led to the development and implementation of additional equipment measures and changes in accident operating procedures with a view to upgrading the functional capabilities of equipment designed for use in ‘complementary domain’ event scenarios; the following subjects were studied for this purpose:

- for actions to be performed in rooms, ease of access to the equipment in question,
- qualification of the equipment for the ambient conditions (temperature, humidity, pressure, irradiation) prevalent in the situations under study,
- reliability of the ‘support’ functions required to perform the tasks for which the equipment is designed,
- ability of the equipment and related procedures to meet the defined objectives.

30.4.6. Taking into account lessons learned during the review associated with the VD3 900 outage for subsequent reviews

The generic studies carried out for the periodic review associated with the VD3 900 outage ran from 2002 to the end of 2008. The lessons learned from this periodic review have, obviously, been used to improve subsequent reviews of French nuclear power reactors. Nonetheless, if the first review of a reactor is both comprehensive in scope and satisfactory in its conclusions, subsequent reviews may be more targeted, for example, they may focus on changes in safety requirements or issues pertaining to the state of structures, systems and components. The operator must nonetheless demonstrate that any analyses that are not reviewed remain valid.

Consequently, the periodic review associated with the third ten-yearly outage of 1300 MWe reactors in France (VD3 1300), for which the periodic review strategic plan was drawn up in 2010, largely focused on the same subjects covered in the review associated with the third ten-yearly 900 MWe reactor outage, in addition to the following new subjects:

- the risk of boron dilution in the RCS during shutdown states,
- a ‘design review’ of the Integrated Digital Protection System-Reactor Protection System (IDiPS-RPS)[857],
- risks pertaining to internal or external electrical interference, in light of the events that occurred at the Forsmark NPP in Sweden in 2006 and at the Dampierre-en-Burly NPP in France in 2007,

[857] Specific to 1300 MWe and 1450 MWe reactors.

- protection from industrial hazards and the risk of an aeroplane crash,
- the lessons learned from Level 1 probabilistic safety assessments that have taken into account not only initiating events inside the reactor, but also internal flooding, fire and earthquake conditions, as well as events that could damage fuel stored in the fuel building pool.

Regarding the N4 reactor series, the generic studies for the first ten-yearly periodic review began in 2007; the first N4 ten-yearly inspections were completed in 2012. The review associated with the second ten-yearly outage (VD2 N4), due for completion in 2021, began in 2011.

The review associated with the fourth ten-yearly outage of 900 MWe reactors (VD4 900) is described in more detail below.

30.5. Fourth ten-yearly outage of 900 MWe reactors: integrating the extension of the operating lifetime of nuclear power reactors in France

30.5.1. Background

In the USA, extending the operating lifetime of nuclear power reactors up to 60 years has been authorized. The first license renewal for a 20-year operating lifetime extension was granted in 2009. By the end of 2013, 40 reactor units had been in operation for over 40 years. A massive investment programme, including replacing heavy components and generally renovating facilities, was implemented.

In Europe, a number of plant operators have initiated programmes to extend the operating lifetime of their nuclear power reactors. EDF, in particular, has launched a wide-ranging programme of investment stretching over two decades to renovate reactors in service in the French nuclear power plant fleet (also known as the 'Major Refit' programme), with a view to extending, under satisfactory safety conditions, their operating lifetime beyond the 40 years for which they were designed (the Operating Lifetime Project). The major changes decided upon following the Fukushima Daiichi nuclear power plant accident (as required by ASN) have been incorporated in this project. For 900 MWe reactors, the most recent 'Phase 3' modifications defined as part of the complementary safety assessments (described in Section 36.6) will be implemented during the fourth ten-yearly outage of these reactors (VD4 900).

More specifically, EDF has set out five key lines of action under the Operating Lifetime Project:

- incorporating international experience feedback in the ten-yearly inspections and safety reviews, including those associated with the fourth ten-yearly outage,
- predicting and managing wear in structures, systems and components,

- using the most advanced technical and technological knowledge,
- planning development of the industrial base,
- maintaining and upgrading the skills base.

The first VD4 900 outage began in 2019 (at Tricastin Unit 1) and the last is scheduled to end in 2030 (Chinon Unit B4).

On the issue of ageing management, it should be mentioned that, in 2008, in order to focus on this subject, EDF set up a research and development institute operating under its coordination, the MAI (Materials Ageing Institute), jointly funded by nuclear power plant operators via the Electric Power Research Institute (EPRI, which represents all nuclear power reactor operators in the USA) and the Japanese company, Kansai Electric Power Company (KEPCO). The MAI has been set up to pool industry expertise to anticipate ageing in NPPs with a view to extending the operating lifetime of facility structures, systems and components. In France, IRSN is conducting research and development studies on the ageing of SSCs[858] to build its expertise in this area.

The stages in the review associated with the fourth ten-yearly outage of 900 MWe reactors are shown in Figure 30.3.

30.5.2. Periodic Review Strategic Plan – Setting objectives

In September 2010, EDF submitted its preliminary plans for the Operating Lifetime Project to ASN. EDF then submitted the generic programme for this project, which was reviewed by IRSN and submitted to the ASN Advisory Committee for Reactors for an opinion. This led ASN to issue a position statement in June 2013, in which it set out three key objectives:

- "the operating lifetime of a nuclear reactor [...] can only be extended if it can be guaranteed that all equipment important to safety shall continue to meet the safety requirements related to it beyond the fourth ten-yearly periodic review [...] in situ testing shall cover all the requirements set out with regard to items important to protection";
- "reactors that are currently in service will exist, worldwide, alongside reactors like the EPR, or equivalent, which are designed to meet significantly more stringent safety requirements. Nuclear reactors must, therefore, be upgraded to align with these new safety requirements, state-of-the-art nuclear technology and the operating lifetime planned by EDF";
- "with regard to safety reassessment, [...] EDF must improve its proposals to further reduce, as far as reasonably possible, the radiological impact of design-basis accidents."

[858] On this subject, see Chapter 10 in Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

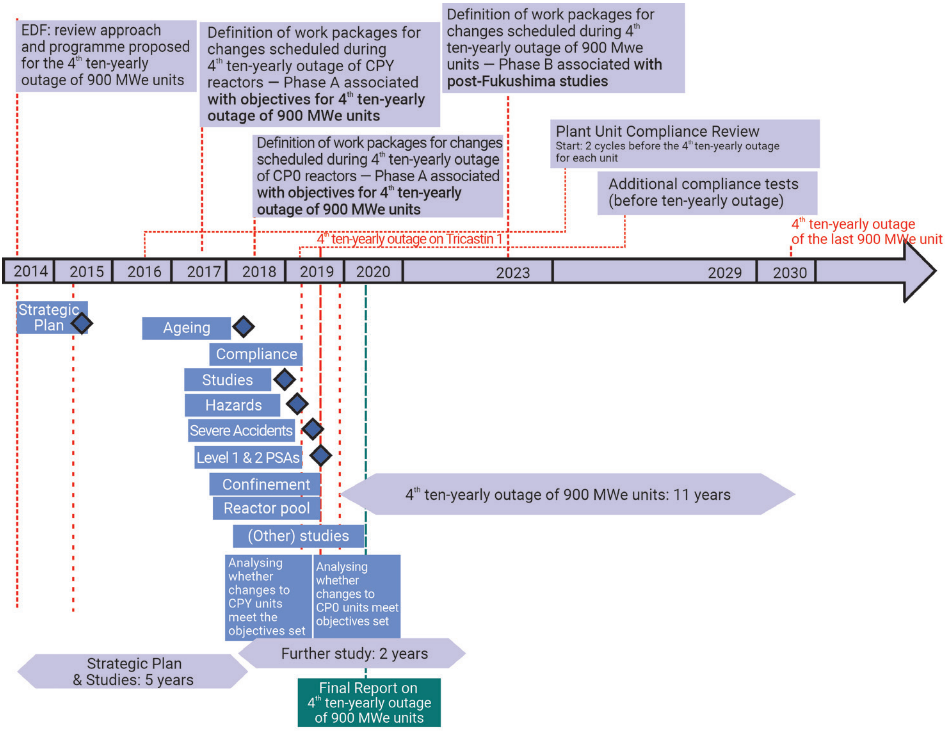

EDF: review approach and programme proposed for the 4th ten-yearly outage of 900 MWe units
Definition of work packages for changes scheduled during 4th ten-yearly outage of CPY reactors – Phase A associated with objectives for 4th ten-yearly outage of 900 MWe units
Definition of work packages for changes scheduled during 4th ten-yearly outage of 900 Mwe units – Phase B associated with post-Fukushima studies
Definition of work packages for changes scheduled during 4th ten-yearly outage of CP0 reactors – Phase A associated with objectives for 4th ten-yearly outage of 900 MWe units
Plant Unit Compliance Review
Start: 2 cycles before the 4th ten-yearly outage for each unit
Additional compliance tests (before ten-yearly outage)
4th ten-yearly outage on Tricastin 1
4th ten-yearly outage of the last 900 MWe unit
2014
2015
2016
2017
2018
2019
2020
2023
2029
2030
Strategic Plan
Ageing
Compliance
Studies
Hazards
Severe Accidents
Level 1 & 2 PSAs
Confinement
Reactor pool
(Other) studies
4th ten-yearly outage of 900 MWe units: 11 years
Analysing whether changes to CPY units meet the objectives set
Analysing whether changes to CP0 units meet objectives set
Further study: 2 years
Strategic Plan & Studies: 5 years
Final Report on 4th ten-yearly outage of 900 MWe units

Figure 30.3. Stages in the review associated with the fourth ten-yearly outage of 900 MWe reactors (the meaning of the symbols is the same as for Figure 30.2). IRSN.

In addition, ASN stated that "EDF's programme should be developed with a view to meeting the objective that all the reactor units [...] that EDF intends to keep in operation after the fourth ten-yearly periodic review must have undergone the work and changes required by the time of the fourth ten-yearly inspection programme."

Regarding the review associated with the VD4 900 outage, EDF submitted the periodic review strategic plan to ASN at the end of 2013[859]. This document presents the generic studies and inspections that EDF plans to perform on all the 900 MWe reactors; it was reviewed by IRSN and by two ASN advisory committees (the Advisory Committee for Reactors and the Advisory Committee for Nuclear Pressure Equipment). ASN issued a position statement on this file in April 2016[860].

Some of the objectives and key points set out for the review associated with the VD4 900 outage are given below:

[859] The report was amended and completed in mid-2014.

[860] Letter setting ASN's position statement, reference CODEP-DCN-2016-007286 dated 20 April 2016.

- in general, the safety reassessment studies associated with the VD4 900 outage must take into account the best international practices, advances in knowledge and changes in the rules applicable to similar types of facility, especially new reactors[861];
- thus, for design-basis (or reference) operating conditions, for 'complementary domain' events and for hazards, the objective is to avoid the need to implement measures for the immediate protection of the public;
- some situations integrated in the EPR design that had not been studied for reactors already in service will now be studied; a 'renovated'[862] complementary domain will be introduced to establish consistency with the EPR safety analysis report;
- measures that have a strong impact on severe accident prevention (water storage and an emergency electrical power supply) will be examined;
- in connection with post-Fukushima studies, measures must be sought to prevent the basemat from being penetrated by corium and to make it possible to remove residual heat from the reactor without having to open the containment filtered venting system associated with the U5 procedure;
- ways should be found to improve performance of the filtration system designed to reduce release if the containment is opened deliberately to depressurize it, if necessary, during a core-melt accident (U5 containment filtered venting procedure); one reason for setting this objective was that IRSN considered that, given technological advances in filtration processes and industrial developments, integrating filter media (such as silver filters) into the U5 system could, in time, help reduce iodine release (in molecular form and organic form), thereby significantly mitigating the radiological impact on people and the environment if it is necessary to vent the containment;
- new equipment installed for managing core-melt situations must be qualified for use under prevailing conditions in these situations;
- regarding spent fuel pools, the risk of fuel melt must be 'practically eliminated';
- the ageing management approach initiated, especially in the context of the VD3 900 outage, must be pursued to include areas in the main primary system made from nickel alloy 600, such as the vessel lower head penetrations, since this material is potentially subject to a stress corrosion phenomenon (see Section 27.2.2.10).

With regard to fire-related risks, ASN asked EDF to substantiate, as part of the VD4 900 outage – in addition to measures already taken subsequent to the VD3 900 outage – that fire compartment design adequately covers all 'fire safety volumes',

[861] For example, ASN Guide No. 22, and documents published by WENRA.
[862] See Section 13.5.

accompanied by a schedule for all related studies and changes. Substantiation[863] must, of course, cover all rooms identified as presenting a high safety risk (based particularly on the fire probabilistic safety analysis).

Following ASN's 2016 position statement regarding the strategy put forward for the periodic review associated with the fourth ten-yearly 900 MWe reactor outage, new position statements were issued at the beginning of 2021, related to ageing management and compliance review. The ASN's position statements are based on IRSN analyses and the positions taken by the Advisory Committee for Reactors.

A few significant issues identified at the end of 2019, some of which are described later in this book, are presented hereafter.

30.5.3. A few significant issues identified in reviews conducted by safety organizations[864]

▶ Plant unit compliance review

For the plant unit compliance review, EDF set out a work programme similar to the programmes deployed for previous reviews, covering various structures, systems and components, including the following:

- civil works structures (effluent retention tanks, essential service water system galleries and pipes, etc.),
- confinement and ventilation systems and structures,
- lifting equipment,
- the main valves used during normal operation for liquid and gas discharges,
- equipment qualified for accident conditions,
- lightning protection systems,
- pipes,
- with regard to seismic hazards, equipment support and anchoring systems,
- fire and explosion protective measures,
- internal and external flooding protective measures,
- local emergency response equipment and resources.

After examining the periodic review strategic plan for the periodic review associated with the VD4 900 outage, and given the compliance deviations that had recently been characterized affecting various SSCs, ASN considered it necessary for EDF to extend

[863] By implementing the 'PEPSSI' method (*Principe d'évaluation pour la suffisance des éléments de sectorisation incendie* – used to assess the adequacy of fire compartmentation), inspired by the EPRESSI method implemented for the Flamanville 3 EPR.

[864] Situation at the end of 2019.

the scope of the plant unit compliance review, as well as the inspection programme included in this review. ASN set out some possible options for the additional inspections, including inspection of the passive systems used in the safety demonstration and equipment designed to prevent and mitigate core-melt situations.

It also became apparent that site inspections should not be limited to visual examinations (without dismantling any equipment) and that, as far as possible, best practices available in the field of inspection should be used.

To meet this requirement, EDF proposed, as part of the ten-yearly outage at Unit 1 of the Tricastin nuclear power plant, carrying out site inspections in rooms that house equipment used directly to allow the unit to reach and maintain a safe state, namely the emergency feedwater system pumps, the essential service water system pumps and the emergency diesel generator engines. These inspections will subsequently be extended to all the 900 MWe reactors in the French fleet, taking into account feedback from this first round of inspections.

Furthermore, following its review of the strategic plan prepared by EDF for the periodic review associated with the VD4 900 outage, ASN reminded the operator that it was important to resolve any deviations, including those which may have only a moderate impact on safety, in order to pursue operation of these reactors. On this point, in 2015 ASN published ASN Guide No. 21 entitled *Traitement des écarts de conformité à une exigence définie pour un élément important pour la protection* (*EIP*) (Processing Deviations from Requirements for Items Important to Protection), which defines procedures for processing deviations and the acceptable time frames within which they must be corrected.

ASN noted that, "if any generic deviation is found, EDF must, as part of its analysis of compliance deviations, state its position regarding the need to extend inspections or accelerate implementation of the inspection programme set out in the plant unit compliance review on other reactors currently in service."

ASN also requested that EDF "improve [its] organization to ensure that any deviations impacting safety identified before the fourth ten-yearly outage of each 900 MWe reactor can be remedied before or during completion of this inspection programme. Any deviations identified during this ten-yearly inspection programme must be corrected as soon as possible, giving due consideration to their impact on safety."

Early in 2018, EDF launched a specific project designed to improve how compliance is managed at its facilities. This project was initiated in the context of the VD4 900 outage, but applies to the entire French nuclear power plant fleet.

▶ Safety reassessment studies

To achieve one of the objectives given above, EDF must address mitigation of the radiological consequences of a steam generator tube rupture, a subject calling for significant improvements to be made in the framework of the VD4 900 outage; this point is developed in more detail in Section 10.3.

Regarding studies pertaining to events in the complementary domain, implementation of the 'renovated' complementary domain has resulted in first, the confirmation of measures already identified in studies on the 'new' complementary domain and second, the choice of using the station blackout diesel generator (SBO DG) as a new complementary domain measure aimed at further reducing risks related to internal reactor events (see Section 13.5).

With regard to preventing the basemat from being penetrated by corium in the event of core melt, EDF assessed different solutions and opted for a strategy entailing dry corium spreading in the (dry) reactor pit, together with corium spreading in the room adjacent to the in-core instrumentation system (ICS); this would be followed by (passive[865]) flooding of corium using water from the reactor building sumps, filled previously using the SIS and CSS systems, or, if they have failed, by the 'hardened safety' core pump.

Regarding research into possible measures for removing residual heat from the reactor in the event of core melt without opening the containment filtered venting system used in the U5 procedure, EDF is planning, as part of Phase 3 of the post-Fukushima changes (see Section 36.6), to install an ultimate CSS system (EASu[866]) designed to remove residual heat released inside the containment.

As part of the VD4 900 outage, EDF is implementing measures for the fuel building that will make it possible to connect an emergency fuel pool cooling system (FPCS 2 – see Figure 30.4), consisting of mobile equipment installed outside the building, which can be used beyond the first 24 h of the event to cool the spent fuel pool if fire or flooding causes lasting damage to the pool cooling system (see Section 15.3).

As mentioned in Section 9.1.4, based on reassessment studies on loss-of-coolant accidents submitted by EDF, the safety organizations considered that additional substantiation was required on achieving core cooling by recirculating water from the containment sumps: further investigation appears necessary to analyse the possible chemical effects induced by the presence of boric acid, sodium hydroxide and dissolved compounds from debris, which may contribute to the risk of clogging not only on sump filters, but also in the fuel assemblies. EDF is planning to conduct additional tests at temperature levels representative of the levels that could be reached in this accident situation.

[865] Achieved by means of a fusible link that breaks when corium comes into contact with it, opening the hatches that let the water flood in.

[866] This system, defined within the context of post-Fukushima changes (see Section 36.6.5.3), consists of a line in the fuel building that is connected to the extraction side of the refuelling water storage tank, consisting of a pump (the hardened safety core pump) and a heat exchanger, which is used to send water into the reactor building and the sumps. The pump is powered by the station blackout diesel generator. The heat exchanger is cooled using the ultimate heat sink (SFu), set into operation by the Nuclear Rapid Response Force.

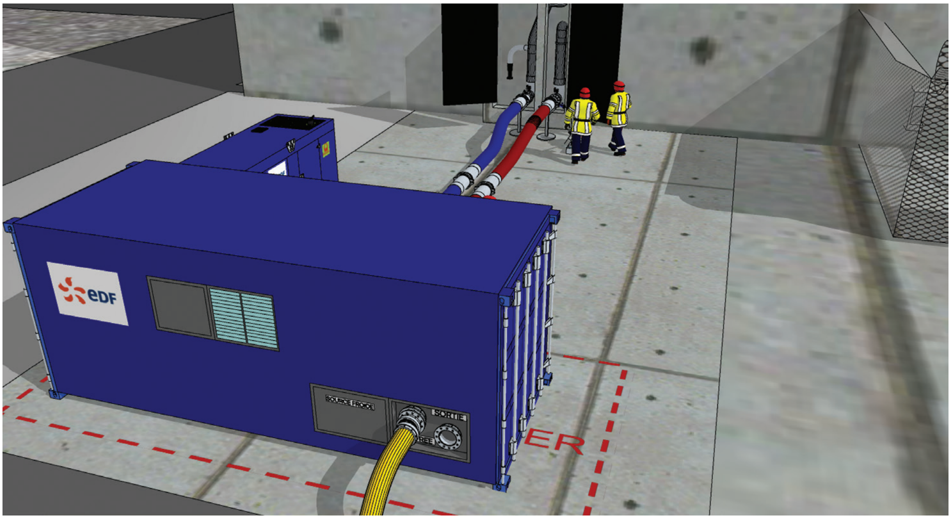


Figure 30.4. Simulation view of FPCS 2, showing the unit housing the pump and heat exchanger in the foreground and the fire brigade hose connections in the background. EDF.

Regarding the probabilistic safety assessments provided to support the periodic review associated with the VD4 900 outage, EDF intends:

- with regard to internal initiating events, to conduct Level 1 PSAs on the risk of fuel melting both in the reactor core and in the stored fuel pool,
- with regard to hazards, to conduct specific Level 1 PSAs on internal fire and flooding, together with in-depth seismic hazard PSAs for those sites considered the most exposed to these types of risk,
- to develop Level 2 PSAs for these three hazard categories – which is an entirely new approach.

Numerous changes, resulting from safety review studies, post-Fukushima studies, and actions required to manage compliance will therefore be implemented. The scale and the combined effect of these modifications will lead to significant changes for workers and organizations present at nuclear power plant sites. Consequently, EDF is implementing a ‘Human and Organizational Factors’ policy, as described in Section 16.2.2.

30.6. Overview of international practices – IAEA Guides

As mentioned earlier in this chapter, the practice adopted in France of holding periodic reviews was not originally introduced to meet regulatory requirements. It was implemented in France gradually – where, starting in the mid-1990s, the review objectives and expected content were specifically defined – as was the case in most countries that operate nuclear power reactors.

30.6.1. International practices

Two documents describing the Periodic Safety Review[867] (PSR) practices implemented in different countries are of interest here:

- an OECD report, issued in 1992, entitled The Periodic Safety Review of Nuclear Power Plants – Practices in OECD Countries,
- and a document published by the IAEA in 2010, entitled Periodic Safety Review of Nuclear Power Plants: Experience of Member States[868].

It is interesting to note that in some countries, when a nuclear power reactor is set into operation, validity of the operating licence may be limited to just a few years, even if the facilities have been designed to last well beyond that period, whereas in France, officially, the operating authorization is not limited in time, as in several other countries, although it must be kept in mind that French reactor units were designed[869] to operate for 40 years. The OECD report mentioned above reveals that, in cases where operating licence validity was short, renewal was generally part of a documentation updating process, sometimes applied annually, involving documents such as safety analysis reports and operational limits and conditions; but the report does not provide details on the purpose of these updates, which is not the case for periodic reviews, where the objectives are known.

In general, it appears that safety reviews were initiated in different countries over the same time span in which periodic reviews were developed in France. These countries saw the advantages of learning from experience and the potential for improving technology. Nonetheless, some other countries, such as the USA, took a different approach, based on specific reactor monitoring and improvement processes, as will be seen further on.

The first safety reviews were carried out on different scales in different countries. Some, involving older reactors, were conducted on a very large scale. This was particularly true in the case of the (gas-cooled) MAGNOX reactors built in the United Kingdom between 1956 and 1971, which included twenty reactor units at eight sites. Long-term safety reviews (LTSRs) were carried out for these units after they had been in operation for 20 to 25 years (i.e. their design-basis operating lifetime) as a condition for extending their operating lifetime. Thereafter, ten-yearly periodic safety reviews (PSRs) were carried out on these units[870].

[867] The expression ‘periodic safety review’ will be used in this section, since it is widely used internationally, including in IAEA standards.

[868] This survey was published in the Technical Document series (i.e. not as a guide), under the reference IAEA-TECDOC-1643, in 2010.

[869] In terms of the lifetime of structures under irradiation, the number of incident transients, etc.

[870] See the HSE report entitled Report by HM Nuclear Installation Inspectorate on the Results of Magnox Long Term Safety Reviews (LTSRs) and Periodic Safety Reviews (PSRs), published in 2000.

The safety reviews conducted in countries other than France – as reported in the two documents mentioned above – were very similar to the safety reassessment part of a French periodic review, giving significant importance to operating experience feedback (including feedback on the accidents at the Three Mile Island and Chernobyl nuclear power plants). 'Additional inspections' were specifically mentioned, however, with regard to the long-term safety reviews of the MAGNOX reactors in the UK, to cover equipment that could be subject to significant ageing (this is included in the compliance review part of French periodic reviews). Insight resulting from probabilistic safety assessments was gradually incorporated into this process. These safety reviews gradually led to significant changes in facilities, for example, the installation of additional generators (as in Germany), additional independent systems for residual heat removal[871] designed to withstand external hazards, including aeroplane crashes (Germany, Switzerland), replacing or adding more reliable safety valves (Belgium, Canada, Italy), improving fire protection measures (Italy), improving the instrumentation used to manage accident situations (Germany, Belgium), modifying reactor cores to reduce the neutron flux received by the reactor vessel (Finland), and changes designed to improve seismic resistance (Italy), etc.

In the USA, targeted review programmes have been conducted at power reactors since the 1970s, for example, the SEP (Systematic Evaluation Process), SSFI (Safety System Functional Inspection), ASP (Accident Sequence Precursor), IPE (Individual Plant Examination), IPEEE (Individual Plant Examination for External Events), SALP (Systematic Assessment of Licensee Performance) launched in 1993, and the review of seismic hazards at all reactor units in the Central and Eastern United States (CEUS) launched in 2012, etc.

Note, however, that since the accident at the Fukushima Daiichi nuclear power plant in March 2011, and following the recommendations made by a U.S. NRC task force, periodic reassessment of seismic and flooding hazards has now been introduced in the USA (see Section 37.5).

30.6.2. IAEA Guides

The IAEA has published several guides specifically covering periodic safety reviews for nuclear power reactors, taking into account feedback on the review process and existing practices. The most recent of these guides is Specific Safety Guide SSG-25 entitled Periodic Safety Review for Nuclear Power Plants, published in March 2013.

This guide points out that, while practices may differ from one country to the next, especially in terms of the scope of the studies and inspections conducted, the main objectives attributed to periodic reviews have converged – except for the US approach, nonetheless recognized as a valid alternative – toward checking for signs of any degradation in facility safety since the previous safety review, and comparing facility safety to levels resulting from the most recent international developments (in technology,

[871] Known as Independent Residual Heat Removal (IRHR) systems.

safety objectives and safety approaches, advances in knowledge and numerical simulation tools, etc.), with a view to identifying any improvements that could be made. The IAEA guide highlights the importance of assessing available safety margins during safety reviews – taking into account any inspections conducted on equipment and revising incident, accident and hazard analyses.

Ten years is taken as the standard review interval, considered to be a period during which sufficient developments will have come about in terms of technical and scientific knowledge, operating experience, the facility environment (population, transport infrastructure, industry ecosystem, natural environment, etc.), organizational changes at the facility, modifications to the facility and changes in its operating procedures, and, lastly, developments in terms of safety objectives, safety regulations and safety standards.

The recommended scope for a safety review is very broad. Based on 14 safety factors, it covers all the safety-related aspects of a nuclear facility, considering not only the structures, systems and components (including auxiliary facilities such as waste storage and treatment facilities, etc.), and their operation, but also all the human and organizational aspects. In the case of the French nuclear power plant fleet, certain safety factors mentioned in the SSG-25 Guide are addressed under specific review programmes covering, for instance, national and international experience feedback, human and organizational factors, safety organization during unit outages, management of service providers and subcontractors, etc.

The IAEA Specific Safety Guide SSG-25 explicitly states that the safety review must include a review for compliance with plant design specifications, performing, as necessary, specific inspections or examinations if the inspection and maintenance programmes in place are considered inadequate for the purpose of assessing whether the plant is capable of functioning safely for at least the period until the next PSR. Practices similar to those implemented in France (compliance reviews, complementary investigation programmes) are thus deployed worldwide.

Last, the IAEA SSG-25 Guide emphasizes the important role that safety reviews can play in supporting an application to renew an operating licence or extending the operating lifetime of a reactor.

30.7. Multilateral practices

In addition to national practices and initiatives held between countries to establish and align recommendations regarding periodic safety reviews, such as those described above, safety assessments conducted under bilateral or multilateral programmes on the safety of nuclear power reactors in service worldwide are invaluable, even if their objectives are not specifically or officially attributed to periodic safety reviews.

Such assessments provide an opportunity to discuss major safety issues affecting facilities in service with the countries or operators involved, taking into consideration their specific design and operating characteristics, including in terms of human and organizational factors, and their national regulatory frameworks. Furthermore, the most recent knowledge, practices, technology, objectives and approaches relating to safety can be used to gain new insights for such discussions, and possibly also suggest improvements to facility safety. Such discussions also contribute to promoting safety culture.

The assessments carried out since the 1970s by the IAEA's Operational Safety Review Teams (OSART) (audits on safety in nuclear facility operations or other nuclear activities) or by RISKAUDIT, the European economic interest group, should also be mentioned. Concrete examples of such assessments are discussed in Section 3.1, focusing, in particular, on reactors in Eastern Europe.

Table 30.1. Timeline and duration of periodic reviews on PWRs.

	VD2 900		VD2 1300		VD3 900		VD1 N4		VD3 1300		VD2 N4		VD4 900	
	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)
1990	🟦													
91	🟦													
92	🟦													
93	🟦													
94	🟦													
95	🟦													
96	🟦													
97	🟦		🟦											
98	🟦	🟩	🟦											
99	🟦	🟩	🟦											
2000	🟦	🟩	🟦											
01	🟦	🟩	🟦											
02	🟦	🟩	🟦		🟦									
03		🟩	🟦		🟦									
04		🟩	🟦		🟦									
05		🟩	🟦	🟩	🟦									
06		🟩		🟩	🟦									
07		🟩		🟩	🟦		🟦							
08		🟩		🟩	🟦		🟦							
09		🟩		🟩	🟦		🟦	🟩	🟦					
2010		🟩		🟩		🟩	🟦	🟩	🟦					
11				🟩		🟩		🟩	🟦		🟦			
12				🟩		🟩		🟩	🟦		🟦			
13				🟩		🟩			🟦		🟦		🟦	
14						🟩			🟦		🟦		🟦	

	VD2 900		**VD2 1300**		**VD3 900**		**VD1 N4**		**VD3 1300**		**VD2 N4**		**VD4 900**	
	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)
15						🟩			🟦	🟩	🟦		🟦	
16						🟩				🟩	🟦		🟦	
17						🟩				🟩	🟦		🟦	
18						🟩				🟩		🟩	🟦	
19						🟩				🟩		🟩		🟩
2020						🟩				🟩		🟩		🟩
21										🟩		🟩		🟩
22										🟩				🟩
23										🟩				🟩
24														🟩
25														🟩
26														🟩
27														🟩
28														🟩
29														🟩
2030														🟩

(1) Period devoted to generic studies for the review and their assessment.

(2) Duration of the outage campaign for the ten-yearly outage conducted on reactors in the series under review.

Chapter 31

Optimizing Radiation Protection and Limiting Doses Received by Workers During Operations in a Nuclear Power Plant

Chapter 1 sets out the principles of radiation protection, namely the justification, optimization and limitation of ionizing radiation doses received by workers and members of the public.

As a reminder, according to the optimization principle in French regulations, individual and collective occupational exposure to ionizing radiation should be kept as low as reasonably achievable[872] below the specified limits.

The aim of this chapter is to illustrate the implementation of this principle by Électricité de France (EDF) on the basis of a few examples of operations carried out in the French nuclear power plant fleet and to mention a certain number of measures taken or considered by EDF for still further reducing the doses received by workers during certain types of operation in future years. Some aspects of the radiation protection optimization process adopted in the EPR design will also be briefly outlined.

Radiation protection needs to be optimized in various contexts: during operations performed to return equipment to a compliant state, during changes made to enhance

[872] As Low As Reasonably Achievable, or the ALARA principle.

reactor safety, during maintenance work and during in-service equipment monitoring operations.

The ALARA approach has been implemented by EDF since the early 1990s to intensify efforts, both by its own operating personnel and by its contractors, to reduce individual and collective doses which, as a result, have on average been divided by a factor of approximately 2 to 3 in 20 years[873]. Figure 31.1 below shows the change in collective dose[874].

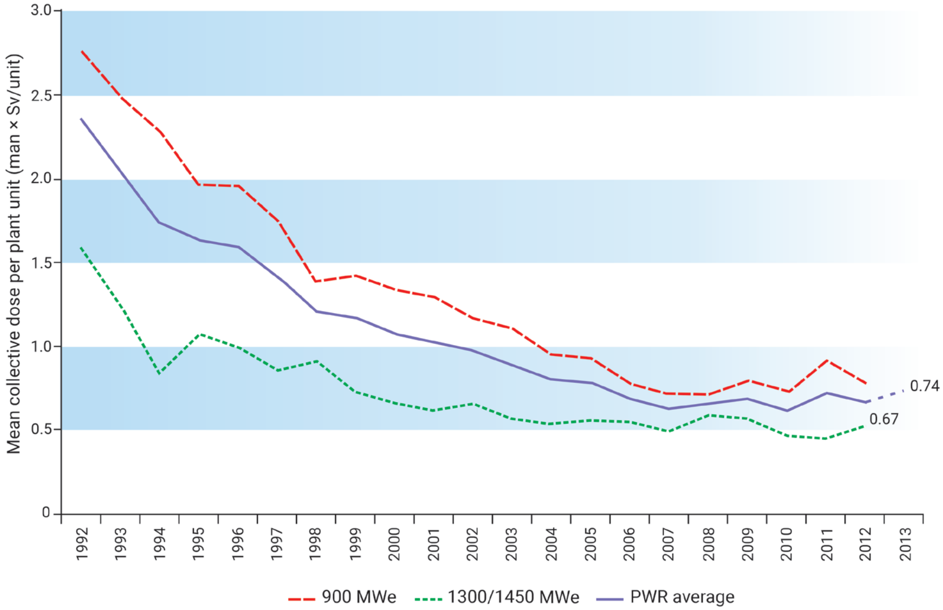


Figure 31.1. Change in mean collective dose per reactor (man-sieverts per reactor) since 1992 (up to the early 2010s) based on operational dosimetry for the fleet and 900 MWe, 1300 MWe or 1450 MWe plant units. IRSN.

31.1. Sources of ionizing radiation in a nuclear power reactor

In an operational (pressurized water) nuclear power reactor, there are three types of ionizing radiation sources:

- **fission products from the fissile nuclei** of uranium-235 together with plutonium-239 in MOX fuel assemblies (see Chapter 5, which recalls a certain number

[873] See EDF *Mémento de la radioprotection en exploitation* (Memento on Radiation Protection in Operations), 2014 edition.

[874] Collective doses are of the same order of magnitude as those in pressurized water reactor fleets of other countries (Belgium, Germany, USA, etc.).

of notions relevant to pressurized water reactor physics). These fission products are mainly iodine-131, xenon-133, krypton-85 and caesium-134 and -137, which may be dispersed in the water of the reactor coolant system in the event of leakage from rod cladding on the fuel assemblies. Fission products emit beta and gamma radiation;

- **activation products** from components (metal structures and their corrosion products, reactor coolant, air, etc.) exposed to neutron flux; the (activated) corrosion products conveyed by the reactor coolant and deposited on the surfaces of the reactor coolant system and auxiliary system components are mainly cobalt-58 and -60 and, to a lesser extent, silver-110m and antimony-124. Activation products emit beta and gamma radiation. They account for over 90% of the doses received by workers, in particular during reactor shutdown periods for maintenance and core refuelling;
- **actinides** composed of heavy nuclei that are present in the fuel loaded in the core or that arise from successive neutron captures; these are primarily plutonium-239 and -240, americium-241 and curium-242 and -244. They may be dispersed in the water of the reactor coolant system in the event of serious damage to the fuel cladding. They emit alpha, beta and gamma radiation as well as neutrons.

31.2. Examples of optimization of worker radiation protection

Some aspects of a worker exposure optimization process, achieved qualitatively and quantitatively, are illustrated below. They are based on two sets of work carried out on reactors in the French nuclear power plant fleet, namely: achieving compliance of the sumps and drainage channels in nuclear auxiliary buildings and waste treatment buildings, and increasing the thickness of reactor basemats at the Fessenheim nuclear power plant.

Work to bring the sumps and drainage channels of nuclear auxiliary buildings and waste treatment buildings into compliance was carried out on all 58 reactor in the nuclear power fleet between 2002 and 2006 in accordance with the Order of 31 December 1999 setting the general technical regulations for preventing and reducing the harmful effects and external hazards resulting from the operation of basic nuclear installations[875]. The need to restore sumps and drainage channels had become apparent following inspections conducted in the course of basic preventive maintenance programmes[876] for civil works (to detect leaks). This work was complex, given the number of operations required, and posed a major radiological challenge, to be achieved within a short period. The radiation sources in the sumps and drainage channels were essentially present in sludge.

[875] Since repealed by the INB Order.

[876] *Programme de base de maintenance préventive*, PBMP.

EDF set up a specific organization for this work under the direction of the Nuclear Power Generation Division (DPN). In addition, the outside contractors involved, providing services in the relevant trades (cleanup, civil and mechanical engineering, painting), formed a temporary consortium for the purpose.

In general, preparation for the work involved:

- breaking down and sequencing the various operations to be carried out,
- estimating the doses that would be received by the workers involved in these operations,
- optimizing radiation protection,
- implementing a process for collecting feedback on lessons learned over the course of the work carried out at the various sites.

The optimization process was developed for the first project carried out on Unit 1 at the Tricastin nuclear power plant in 2002. This resulted in a generic optimal scenario and identified additional approaches to optimization. Thirty-six options (or ‘good practices’) were thus examined in four areas:

- reducing the number of radiation sources,
- providing biological shielding,
- working from a distance,
- optimizing the time required to complete the operation.

Of the 36 options examined, ten were rejected because the anticipated gains in terms of operator doses were slight in comparison with the drawbacks. To illustrate, some of the options investigated and the consequent decisions are listed below:

- partially opening the drainage channels to facilitate access during operations, flooding sumps adjacent to the work areas with water; these two options, capable of reducing ambient dose rates for operators, were selected;
- chemical decontamination of the pipes in the safety injection system (SIS) and chemical and volumetric control system (CVCS) to reduce ambient dose rates at workstations; this option was not selected because it was difficult to implement;
- wetting the sludge, in particular to avoid dispersal of substances; this option was not selected because it would also have resulted in wetting and contaminating the concrete;
- using poles to suction the sludge; this option, capable of reducing operator doses, was selected;
- robotic decontamination of the inside of the sumps; this option was not selected due to difficulty in implementation (handling a contaminated system, storage of radiation-emitting equipment, no time savings due to robot manoeuvring, etc.).

Another example is the work performed to increase the thickness of the basemat on both units at the Fessenheim nuclear power plant, which was recommended in 2011 by the French Nuclear Safety Authority (ASN) in a decision pertaining to continued operation of these units after their third ten-yearly outage (900 MWe reactors of the CP0 group, commissioned in 1978). This is because it had become apparent that, in certain core-melt accident scenarios with vessel melt-through, corium could pass through the basemat of these units in less than 24 h. The selected additional thickness was 50 cm, taking the thickness of each basemat from 1.5 m to 2 m. The selected solution provided for corium to spread via a transfer tunnel into a zone adjacent to the reactor pit.

Given the prevailing radiological conditions in the reactor pit, this operation could only be carried out during shutdown of the reactor in question after complete core defuelling.

EDF implemented an optimization process capable of reducing the initially estimated collective dose of 280 man-millisieverts to 90 man-millisieverts. The various operations to be carried out and their duration were determined in greater detail using a full-scale mock-up of the work area in a reactor. Selection of a self-levelling concrete made it possible to reduce work time in the reactor pit. Furthermore, to avoid damaging the reactor in-core instrumentation system (RIC system), featuring measurement tubes that are routed through the lower part of the reactor pit, the neutron probes were withdrawn during the work (this withdrawal operation involved additional exposure that was offset by dosimetric gains obtained during work to increase basemat thickness). The operations carried out in each reactor resulted in the operators receiving an actual collective dose of 72 man-millisieverts.

31.3. Arrangements for 'Major Refit' operations

In 2010, EDF decided to initiate a large-scale operation, referred to as the 'Major Refit', to renovate all the reactors in the nuclear power plant fleet in order to extend their operating lifetime beyond 40 years. The aim is twofold:

- first, to anticipate and manage equipment ageing by monitoring its state of wear and, if necessary, replacing it;
- second, to upgrade facility safety and bring it to a level comparable with that intended for future reactors; the safety objectives set by EDF mainly involve reducing the probability of core melt and mitigating radiological impact in the event of an accident.

The corresponding renovation work involves several items of equipment and systems, including:

- steam generators, which continued to be replaced if they were equipped with alloy 600 tubes[877] (900 MWe and 1300 MWe reactors),

[877] See Section 27.3.

- changes decided in the context of the periodic reviews associated with ten-yearly outages (fourth ten-yearly outage for 900 MWe reactors, third ten-yearly outage for 1300 MWe reactors and second ten-yearly outage for 1450 MWe reactors),
- operations involving application of regulations on nuclear pressure equipment,
- changes arising from the complementary safety assessments carried out in the aftermath of the Fukushima Daiichi nuclear power plant accident in March 2011.

This work is to be carried out in both the conventional part and the nuclear island of the power plants, and thus in some cases on systems conveying radioactive fluids or in the vicinity of these systems. In order to determine the impact of this work on worker radiation protection (for both EDF and contractors' personnel), EDF assessed the scope and the increase in volume of the operations to be carried out in the facilities, and the radiation protection issues relative to the operations and practices previously implemented during unit shutdowns.

This assessment, carried out in 2013, suggested that the work would result in a significant increase in the volume of maintenance and hence in the associated doses received over the 2015-2025 period. An update to this assessment, carried out two years later by EDF, revealed a distinctly less significant increase in forecast doses (see Figure 31.2) as a result of spreading the work out over time and leveraging radiation protection optimization.

The measures taken by EDF, both organizationally and technically, to optimize radiation protection during reactor renovation operations were submitted and discussed with the safety organizations in 2015. This offered an opportunity to appraise EDF's radiation protection practices, performance and the lessons learned from operating experience since the early 1990s.

The analysis emphasized the significance of the following organizational factors in radiation protection:

- rapid response processes:
  - feedback processed quickly after events involving radiation protection issues,
  - knowledge leveraged, updated and disseminated quickly and regularly, good radiation protection practices implemented at facilities,
  - 'predictable' degraded situations and co-activity situations incorporated in risk analyses;
- contractors involved in optimization studies;
- on completion of the first unit outages in the reactor renovation project, checking that the personnel appointed as 'area supervisors' (a recently created support and advice function at the interface between logistics and risk prevention) are sufficient in number and have the required skills.

On a technical level, the chosen objectives and measures include:

- replacing materials coated with stellite[878] (hard, cobalt-based material) as far as reasonably possible;
- reducing point-source contamination by silver-110m and antimony-124[879];
- electrochemical polishing of steam generator channel heads. The reduction in surface roughness means that fewer activated corrosion products are 'caught' on the surfaces; this brings about a significant dose rate gain in channel heads and, to a lesser extent, in dose rates at the steam generator floor level. All replacement steam generators (new equipment) undergo this operation;
- continued optimization of reactor coolant chemistry to reduce the quantity and radioactivity of the corrosion products present in the reactor coolant (injection of zinc acetate, high-throughput purification of reactor coolant in shutdown phase, increase in hydrogen content in water to reduce the risk of stress corrosion, etc.);
- implementing the most effective curative measures involved in clean-up and tracking down 'hot spots'[880] (whether in reactors or in the spent fuel pools);
- making increased use of remote-controlled operations (including remote-controlled pipe welding technology in replacing the 1300 MWe reactor steam generators).

The examination carried out in 2015 also provided an opportunity to analyse prospects for optimizing and reducing doses for the various tasks considered the most 'dose-intensive' and the 'specializations' with the greatest exposure. These tasks mainly involve replacing:

- steam generators,
- pressurizer heaters,
- rod cluster control assembly (RCCA) guide pins,
- RCCA drive mechanisms,
- the 'tee' section of the residual heat removal system (RHRS).

The specializations with the greatest exposure are mainly those whose work involves thermal insulation or scaffolding, together with mechanics, welders, valve specialists and gamma radiographers (who take X ray images).

[878] This material is present in the form of coatings or solid hard parts in contact areas with demanding functional requirements in terms of leaktightness, frictional guidance or sliding.

[879] Silver is found in the neutron-absorbing alloy AIC (Ag-In-Cd) used for control rod assemblies or in Helicoflex seals; antimony is a component of secondary 'source rod assemblies' (or formerly in graphite-based end stops and bearings in auxiliary system pumps).

[880] A 'hot spot' is a point source, generally composed of active cobalt-60 particles, which, in its immediate vicinity, generates a dose rate much higher than the ambient dose rate in the area. EDF has compiled documents on good practices for eliminating these 'hot spots'.

The potential for making more general use of selenium-75 for gamma radiography[881], instead of iridium-192, for example, has been examined, with the additional advantage of image quality being better with selenium-75. This radionuclide also has advantages in terms of radiation protection (at identical source activity, the dose rate [in mGy/h] at 1 m for a selenium-75 source is divided by 2.5, in relation to that of an iridium-192 source), but, due to its characteristics, it cannot be put to general use in gamma radiography since it can only be used effectively for metal structures that are no thicker than 30 to 40 mm. While EDF is pushing to expand the use of this radionuclide in gamma radiographic inspections, supply difficulties and the high cost of the sources as well as regulatory restrictions[882] mean that on-site use still remains limited.

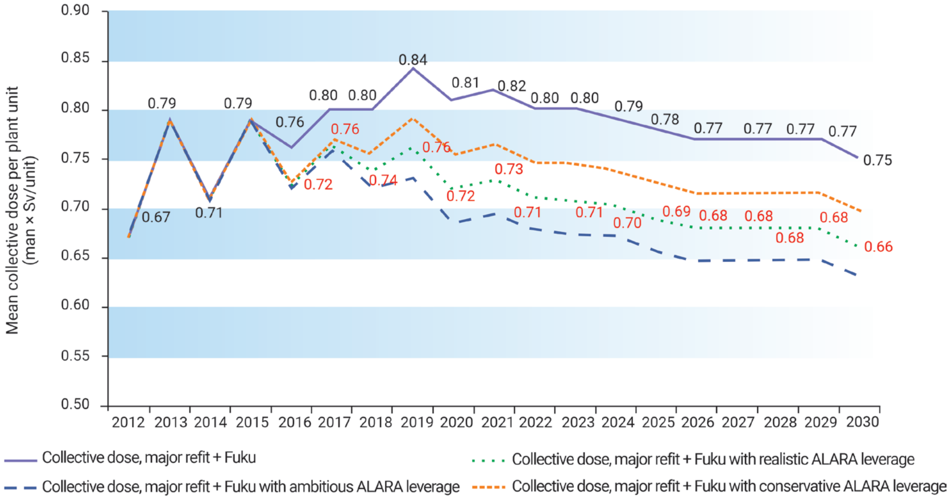


Figure 31.2. EDF's presentation of the effects of radiation protection 'leverage' options on collective dose paths estimated in 2015 ('Fuku' denotes post-Fukushima measures). IRSN (source EDF).

31.4. Approach and objectives adopted for the EPR

In relation to the EPR, general safety and radiation protection objectives were selected back in the 1990s for the design of next-generation reactors and were combined in the Technical Directives issued in the early 2000s (see Chapter 18); these objectives include reducing collective and individual doses relative to fleet reactors already in operation. An optimization process was implemented at the EPR design stage by the designer Areva-NP and by EDF on the basis of the dosimetry records from the operating fleet, in particular those relating to the 'best' 1300 MWe (P'4 series) and

[881] Readers may also consult Current State of Research on Pressurized Water Reactor Safety by J. Couturier and M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2018, section 10.1.2.

[882] The design and construction rules for mechanical components (RCC-M) does not specify the use of selenium-75.

1450 MWe (N4 series) reactors. Priority was given to those activities that contribute to the highest collective doses, for example:

- fitting and removing thermal insulation,
- opening and closing the reactor vessel,
- preparing and inspecting steam generators,
- worksite logistics,
- valve-related activities,
- fuel removal,
- radioactive waste packaging.

EDF thus estimated that the target collective dose could be reduced from an initial reference value (on the basis of operational feedback from the fleet in operation) of 440 man-millisieverts per reactor and per year to 350 man-millisieverts by taking into account the design optimization process carried out for these activities; EDF furthermore set the objective of ensuring that, in normal operation, personnel would not be exposed to the risk of internal exposure.

Special attention has been given to specific design arrangements for the EPR in the optimization process, such as the 'two room' concept, conceived to allow personnel to work in the reactor building outside of unit outages, especially when preparing for these outages (seven days before shutdown). In order to limit exposure for the workers involved, the reactor building is divided into an 'equipment area' (consisting of the main components in the reactor coolant system) and a 'service area' equipped with appropriate biological shielding and where the atmosphere is compatible with the presence of people during operation.

Moreover, choosing to have core neutron instrumentation passing through the head of the vessel, and not through the bottom, is another example of a design choice which will contribute to reducing the doses received by operators.

The EPR design also benefits from a significant reduction in the inventory of cobalt that could be activated during operation.

With regard to equipment design, apart from a reduction in the use of hard coatings capable of generating cobalt-60, the optimization process carried out by EDF has also led, for example, to the design of thermal insulation that can be fitted and removed quickly, and to electropolishing the steam generator channel heads and other parts to limit irradiation and contamination risks for personnel.

Operation of the Flamanville 3 EPR will make it possible to assess whether the optimization process carried out at the design stage (leveraged by operational optimization measures) has indeed produced the expected results and will provide an opportunity to make any necessary corrections or improvements.

Video available for viewing

Controlled Areas: Radiation Protection in Nuclear Facilities

Part 4

The Accidents at Three Mile Island, Chernobyl and Fukushima Daiichi Nuclear Power Plants, Lessons Learned and Emergency Response Management

Chapter 32
The Three Mile Island Nuclear Power Plant Accident

The core-melt accident that occurred on 28 March 1979 at Unit 2 of the Three Mile Island nuclear power plant in the USA sent shock waves around the world, making professionals in the nuclear industry suddenly realize that they needed to totally rethink the risks involved in operating a nuclear power reactor.

Prior to the accident, no one had ever thought that the core of a nuclear power reactor could actually melt, and especially not in such a short period of time, even if the possibility of core melt and the events that could lead up to it had been explored in some studies, including some conducted in the USA[883]. After the accident, once it became possible to look inside the damaged reactor core, it was found that nearly half the core had melted and that about 20 tonnes of molten material had flowed down into the lower head of the reactor vessel. Analysis of the accident also revealed that the entire accident sequence took just under four hours, and that, fortunately, reactor vessel integrity was not lost on contact with the molten material and the containment was not damaged.

These studies raised a whole series of questions regarding the phenomenology of core-melt accidents, as described in Chapter 17.

[883] These studies include those on which the WASH reports were based: the WASH-740 report published in 1957, followed by the more widely-known WASH-1400 report, drawn up at the request of the US nuclear safety authority under the direction of Professor Norman Rasmussen and published in 1975.

The accident at Three Mile Island led to large-scale analytical research, as well as a great deal of international debate and an in-depth review of the risks and the safety approach applied to nuclear reactors.

This chapter describes the accident sequence, its consequences and some of the key lessons learned.

Given that the accident occurred in a type of reactor that is widely used around the world (pressurized water reactor), many countries were involved in the effort to establish the sequence of events and analyse the physical characteristics of the accident. Their studies were based on interpretation of the data recorded by the plant instrumentation systems during the accident, knowledge of the final degraded state of the reactor core as observed when the reactor vessel head was opened at the end of 1984, i.e. five years after the accident, examination of the debris extracted from the core carried out at hot labs, and the use of simulation codes to reconstruct the accident scenario. Collaboration between specialists has, in particular, helped further understanding of thermal-hydraulic phenomena that occurred in the reactor core and reactor systems during the accident, as well as the different stages involved in core degradation. These subjects are described in detail in the study on core-melt accidents in power reactors[884] published by IRSN. Readers who wish to learn more about these aspects are invited to read the book; this chapter discusses only a few of the essential aspects covered in the book. Other sources[885] have also been consulted.

32.1. Accident sequence – Reconstitution through simulation

The Three Mile Island nuclear power plant in Pennsylvania (USA) is located on the Susquehanna River, 16 km from the state capital, Harrisburg, which, at the time of the accident, had a population of 90,000 people. It had two 900 MWe pressurized water reactors designed by Babcock & Wilcox. Unit 2 at the site was brought into commercial service on 30 December 1978.

Pressurized water reactors designed by Babcock & Wilcox broadly resemble the Westinghouse pressurized water reactors in operation in France (see Figure 32.1). They differ from the reactors in France on two key points involving operation and safety: they only have two reactor core coolant loops, whereas the French units have three or four coolant loops, and the steam generators are straight-tube, counter-flow

[884] Nuclear Power Reactor Core Melt Accidents – Current State of Knowledge, D. Jacquemain et al., Science and Technology Series, IRSN/EDP Sciences, 2015, chapter 7.

[885] The Need for Change – The Legacy of TMI, Report of the President's Commission on the Accident at Three Mile Island, Government Printing Office, Washington DC, Kemeny, J. G., Babbitt, B., Haggerty, P. E., Lewis, C. D., Marrett, C. B., Mc Bride, L., McPherson Jr, H., Peterson, R., Pigford, T. H. and Trunk, A., 1979, and Three Mile Island: a Report to the Commissioners and to the Public, Vol. 1, Nuclear Regulatory Commission, Rogovin, M. and Frampton, G. (1980) and *L'accident de la centrale nucléaire de Three Mile Island* (The Accident at the Three Mile Island Nuclear Power Plant) by M. Llory, 1999, *Éditions L'Harmattan*, Paris.

heat exchangers, whereas the steam generators used at French PWRs have U-bend tubes. There were two such steam generators for each reactor unit at the Three Mile Island plant and they were taller, implying a different system layout and complicating circulation of the reactor coolant by natural convection. Very little water was contained in the secondary line; if the feedwater to the secondary line is stopped, this type of steam generator will dry out in two to three minutes, whereas dryout in a steam generator with U-bend tubes takes about ten minutes. Low thermal inertia leaves facility operators with less flexibility in facility control.

The accident was initiated on Wednesday, 28 March 1979, at 4 a.m., with a relatively ordinary operating incident: a failure in the main feedwater system prevented feedwater supply to the steam generators while the reactor was at full power. This failure was probably caused by an error that occurred during maintenance work on the auxiliary systems.

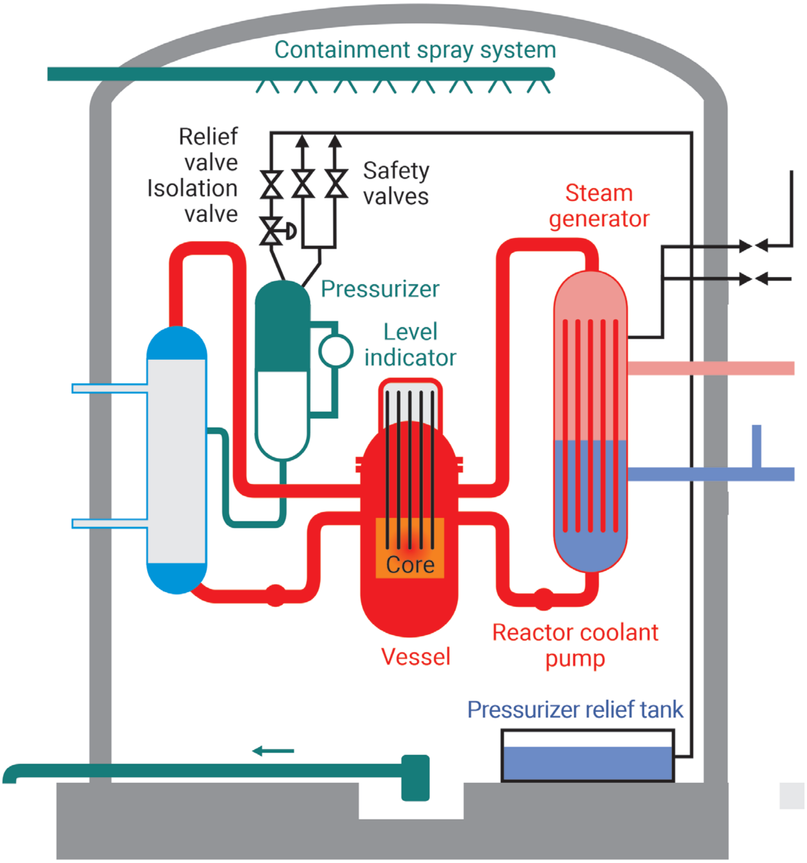


Figure 32.1. Diagram of TMI 2. Georges Goué/IRSN.

The sudden loss of heat removal through the steam generators then led – within a matter of seconds, due to low thermal inertia in the steam generators – to a temperature rise in the cold legs and a pressure rise in the reactor coolant system. Just as it is designed to do in such a situation, the relief valve leading out of the top of the pressurizer opened to lower the pressure in the RCS, discharging coolant into the pressurizer relief tank, which is located inside the reactor containment.

This transient also rapidly tripped the reactor, leading it to shutdown.

Twelve seconds later, the relief valve at the top of the pressurizer received the command to close.

On the secondary side, the transient tripped the turbine generator and started up the steam generator emergency feedwater pumps.

There was nothing abnormal about this first stage of the accident: all the automatic systems functioned perfectly.

But then two equipment failures occurred:

- the pressurizer relief valve, having received the command to close, remained open; coolant therefore continued to flow into the pressurizer tank located inside the reactor containment;
- the steam generator emergency feedwater system (EFWS) pumps started up after 30 s, but the water was kept from reaching the steam generators, since the valves on the lines running between the pumps and the steam generators were closed when they should have been open (they had been closed during a regulatory test performed a few days earlier); the secondary side of the steam generators then drained out within two or three minutes, leading to a loss of cooling in the RCS by the steam generators.

This initial failure had serious consequences because the operators in the control room were not aware that the pressurizer relief valve had remained open; for over two hours, approximately 60 t/h of coolant spilled into the containment (the RCS contains approximately 200 tonnes of coolant). The operators failed to realize that the relief valve was jammed open because there was no instrumentation in the control room to indicate the actual position of this valve, only a light on the control room panel indicating that a command had been sent to close the valve; they therefore had no way of knowing that the valve had not closed.

The second failure may not have had a major influence on the sequence of events. However, even though the position of the valves on the emergency feedwater system supplying the steam generators was indicated in the control room, the operators did not identify the fault for another eight minutes, at which point they gave the order to open these valves manually. For almost 25 min, the operators' attention was primarily focused on performing manoeuvres to stabilize cooling conditions on the secondary side, which may partly explain why they did not understand the early critical stages of what was happening in the RCS.

What exactly was happening in the reactor coolant system? After opening the pressurizer relief valve, pressure in the RCS fell to approximately 110 bars within two minutes. The high-head safety injection system then started up automatically, sending cold water into the reactor coolant system.

At this point, the operating crew was concentrating on watching the level of coolant in the pressurizer. Under normal operating conditions, with the relief valve tightly closed, the operator must comply with the instruction to keep the steam bubble at the top of the pressurizer, which implies making sure that the level of liquid in the pressurizer does not vary too much, a sign that pressure is stable inside the reactor coolant system. If the pressurizer fills to the top with reactor coolant, the operator no longer has the steam blanket required to control pressure; the reactor coolant system is then completely flooded with coolant and any transient that occurs will cause sudden variations in pressure, jeopardizing RCS containment integrity.

But the water level inside the pressurizer, after initially falling when the pressurizer relief valve was opened, began to rise rapidly for about six minutes after the reactor trip. This rise in the water level was due to the fact that the pressurizer relief valve had remained open and that the safety injection system was sending water into the reactor coolant system at high pressure.

Believing that the relief valve was closed, the operators interpreted this rapid rise in water level in the pressurizer as being due to the water injected via the safety injection system, and assumed that this injection would cause pressure in the RCS to rise again. Fearing that too much water was being injected into the RCS, they took the decision – which had the most serious repercussions – to manually stop the safety injection system (after less than five minutes of operation).

The mental representation that the operators had was due to an error in the information available in the control room; but this picture served as the basis for the action that they took.

From that moment on, the water leaking from the RCS through the pressurizer relief valve was no longer being replaced, as there was not enough makeup water entering via the chemical and volume control system. In reality, the operators were faced with a loss-of-coolant break situation with total shutdown of the safety injection system.

The reactor coolant slowly filled the pressurizer relief tank. About a quarter of an hour after initiation of the accident, the rupture disc at the top of the tank burst, allowing coolant to overflow directly into the containment building. At that time, the volume of coolant lost through the break and the drop in pressure caused steam to form inside the reactor coolant system.

The RCS was then filled with a mixture of water and steam, with the steam fraction increasing over time. In spite of a number of indications (increased neutron flux in the core, vibrations in the RCS pumps, rising water level in the pressurizer relief tank, high pressure and temperature inside the containment) and alarms which might have alerted the operators to the conditions in the RCS, they kept the RCS operating under these conditions for over an hour. The heat produced by residual heat in the core was being removed partly by the steam generators – the operators did succeed in restarting the emergency feedwater system to the steam generators – and partly by the water and steam running down to the containment floor through the open pressurizer relief valve – but the operators were unaware of this.

The pressurizer was filled with a mixture of water and steam. The level indicated by the instrumentation made no sense.

The steam fraction in the coolant was increasing. The RCS pumps, operating under greater and greater strain, were cavitating and vibrating.

One hour and 13 min after the beginning of the accident, with the vibrating becoming excessive, the operators shut off one of the main reactor coolant pumps, followed by the second 27 min later. It was then that, given the pressure and temperature readings from inside the reactor containment, the operators began to suspect that there might be a leak in the reactor coolant system on the steam generator side. They were hoping that the coolant in the system would start to circulate by natural convection and thus cool the reactor core.

In fact, what happened was that shutting down the main reactor coolant pumps caused the steam and water to separate in the RCS. The steam rose to all the high points in the RCS, while the water dropped to the low points. The coolant was no longer circulating through the system, so no more heat was being exchanged between the reactor core, which was releasing several megawatts of residual heat, and the steam generators. According to post-event analysis, at that moment, the coolant level was close to the top of the core.

The reactor was only being cooled by fluid coming from the chemical and volume control system. This was not enough to make up for the amount of coolant being lost through the pressurizer relief valve. The level of coolant in the reactor vessel was therefore dropping.

Data pertaining to the state of the fuel rods and reactor core, as well as a certain number of phenomena produced inside the core, determined by post-event reconstitution of the accident based on calculations and observations made at a much later time, are shown in green in the account of the sequence of events[886] that follows.

> It is estimated that uncovery of the fuel rods began 1 h and 52 min after the beginning of the accident (at which time the coolant level was at the top of the fuel rods in the core). Due to inadequate cooling, the rods then began to heat up.
>
> It is also estimated that between 2 h and 10 min and 2 h and 20 min after the beginning of the accident, temperatures in the upper sections of the fuel rods rose

[886] This data is based on Nuclear Power Reactor Core Melt Accidents – Current State of Knowledge, D. Jacquemain et al., Science and Technology Series, IRSN/EDP Sciences, 2015, chapter 7.

to 800°C, causing the Zircaloy cladding to swell and rupture, releasing gaseous fission products through the break in the RCS and into the containment.

Two hours and 14 min after the beginning of the accident, the 'high-level in-containment radioactivity' alarm was triggered. The operators were forced to recognize that the situation was serious.

Two hours and 22 min after the beginning of the accident, realizing that it was possible that radioactivity was being released via the pressurizer relief valve, which had been leaking at a high rate even before the accident, the operators closed an isolation valve upstream of the relief valve, thereby eliminating the break in the RCS.

However, this also stopped heat removal (since the RCS and the safety injection system were shut down). Up until 2 h and 54 min after the beginning of the accident, nothing had been done to cool the reactor core other than to use the chemical and volume control system.

Due to exothermic oxidation of the Zircaloy fuel cladding by the steam, releasing more heat than the decay heat from the core while also producing hydrogen, temperature in the core continued to rise. The release of hydrogen and the additional steam produced due to heating of the core caused pressure to rise in the RCS, which, now that the isolation valve on the pressurizer relief line had been closed, was now totally sealed.

The water level in the core continued to drop until it was covering only one metre of the total fuel rod length of 3.6 m. With the water level continuing to fall, and the oxidation reaction propagating across the uncovered parts of the cladding, temperature in the core continued to rise, damaging the core and resulting in molten metal material starting to flow downwards toward the lower head. As this molten material reached the interface between coolant and steam, it solidified on contact with the coolant, forming a crust made up of molten material and solid fragments that had dropped from above. Since the materials accumulating in this crust were not cooled, they gradually heated up, melting in the centre to form a pool of molten material.

Two hours and 54 min after the beginning of the accident, the operators restarted the main reactor coolant pump on one of the cooling loops in an attempt to re-establish circulation of the coolant. In just 6 min, 28 m^3 of cold water were injected into the reactor vessel – the largest injection of coolant since the main reactor coolant pumps were shut down.

This resulted in a rapid pressure rise in the RCS, due to water turning to steam on contact with the overheated elements in the reactor, as well as rapid oxidation of the Zircaloy cladding that had not yet oxidized in the upper half of the core, and, most probably, degraded heat exchange conditions in the steam generators caused by hydrogen produced as a result of Zircaloy oxidation. This injection of water most likely prevented a pool of molten material from developing on top of the crust. Nonetheless, the thermal-mechanical stress generated as a result of quenching what remained of the oxidized fuel rods at the top of the reactor core caused oxidized cladding and fuel pellets to fragment. This then formed a mass of several tonnes of compacted debris on top of the materials already contained in the crust.

The operators stopped the main reactor coolant pump six minutes after starting it back up because of a sudden pressure spike in the RCS. This pressure spike also made the operators re-open the isolation valve on the pressurizer relief line. That set off a new series of radioactivity alarms, some of them outside the reactor building. At that point, the first two confinement barriers had failed and the reactor building (reactor containment) had still not been isolated.

The water flooding into the reactor building was being collected by the automatic containment sump (floor drain) pumps which then pumped the contaminated water in the sumps to storage tanks located in a non-leaktight auxiliary building (see Figure 32.2). These storage tanks then overflowed and contaminated water flooded into the auxiliary building, from where it was released to the environment outside the power plant.

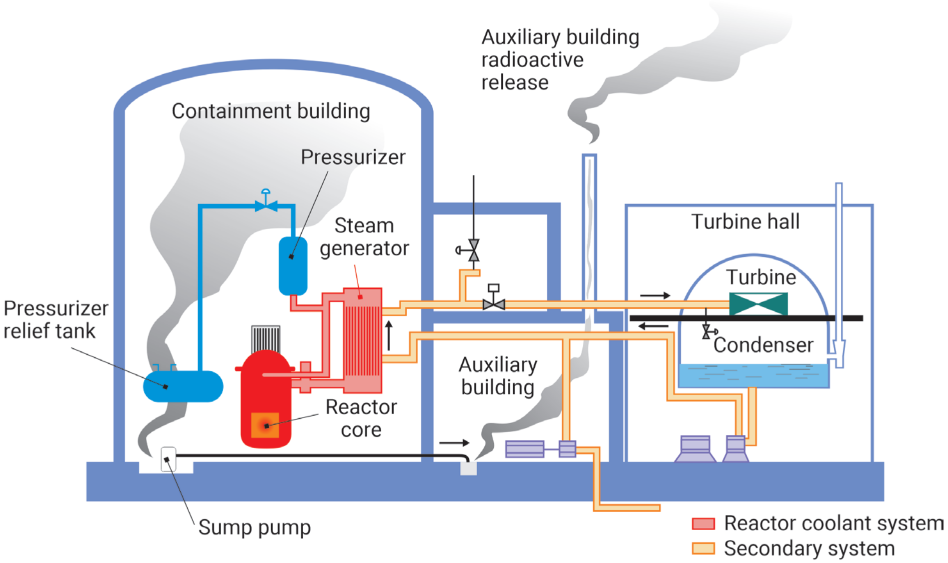


Figure 32.2. Radioactive release pathways. Georges Goué/IRSN.

An emergency situation was finally declared. The reactor containment was isolated, stopping the transfer of radioactivity from the sumps to the auxiliary building. This was 3 h and 20 min after the accident had begun.

The amount of water in the reactor vessel decreased in the 20 min since they had stopped the main coolant pump, as the water boiled and turned to steam due to the decay heat.

The operators then restarted the high-head safety injection system for 17 min, first at a reduced rate, and then at nominal rate.

> Seven minutes after starting up this system, the reactor vessel was filled with water. However, according to post-event estimates, by the time that safety injection restarted, the pool of molten material was already too large for it to be cooled.

Three hours and 44 min after the beginning of the accident, while the operators were focused on cooling the reactor core – which they did not believe to be severely degraded –, a number of instrument readings suggested that there was some movement of the fuel in the core. It was only much later, after examining the lower plenum of the reactor vessel, that the sequence of events could be reconstituted: the crust had eventually given way at one side and 20 tonnes of molten material had flowed down into the lower head of the reactor vessel, destroying the internal structures around the edge of the core along the way.

Within a few hours, the water present in the reactor vessel finally cooled and solidified the molten material. The reactor lower head withstood the flow of molten material. One possible explanation for this was the existence of a gap between the molten material and the vessel wall, which may have allowed water or steam to circulate, thus reducing heat transfer to the vessel.

Water was kept from entering the reactor coolant system by non-condensable hydrogen and fission gases, which it took another 12 h to remove. This was achieved by alternately opening and closing the pressurizer relief line, and using the main coolant pumps and the safety injection system. This released hydrogen and radioactive fission products into the reactor containment.

About nine and a half hours after the accident had been initiated, hydrogen combustion (an estimated 320 kg hydrogen had burned) caused a pressure spike of approximately 2 bars inside the reactor building. The containment was designed to withstand 5 bars, so containment integrity was not lost. However, on entering the reactor building a few months later, it was found that some parts of the internal structures in the building had been damaged by fire and pressure.

Eleven hours and 8 min after the beginning of the accident, the isolation valve on the pressurizer relief system was finally closed, thereby stopping the release of radioactive substances into the empty space inside the containment.

Thirteen hours and 23 min after the beginning of the accident, operators restarted safety injection to refill the RCS.

Fifteen hours after the beginning of the accident there was enough water in the RCS to restore coolant recirculation. Normal and stable cooling conditions were thus obtained about 16 h after initiation of the accident. Twenty-four hours after the accident began, the main coolant pumps were stopped again, as natural circulation between the reactor vessel and the steam generators had been restored, making it possible to remove decay heat from the reactor core.

It took several more days to rule out any possibility that a hydrogen explosion might occur inside the reactor vessel, which was one of the main concerns of the emergency response management teams and the authorities (see the study by M. Llory mentioned at the beginning of this chapter).

32.2. Accident consequences

The plant suffered considerable internal damage. However, this was seen not until 1985, more than five years after the accident, when it became possible to send a camera in between the lower internal structures of the core and the reactor vessel: almost half the fuel had melted, taking cladding and structural materials with it, 62 tonnes in all, to form what is known as 'corium'. Part of this fell to the reactor vessel lower head, fortunately without breaking through it (Figure 32.3); nearly half of the gaseous and volatile fission products (krypton, xenon, iodine and caesium) contaminated the reactor coolant, which reached a radioactivity level of nearly 3 × 10^{16} Bq/m^3, and over 2000 m^3 of this radioactive water had leaked out of the RCS and flooded into the containment.

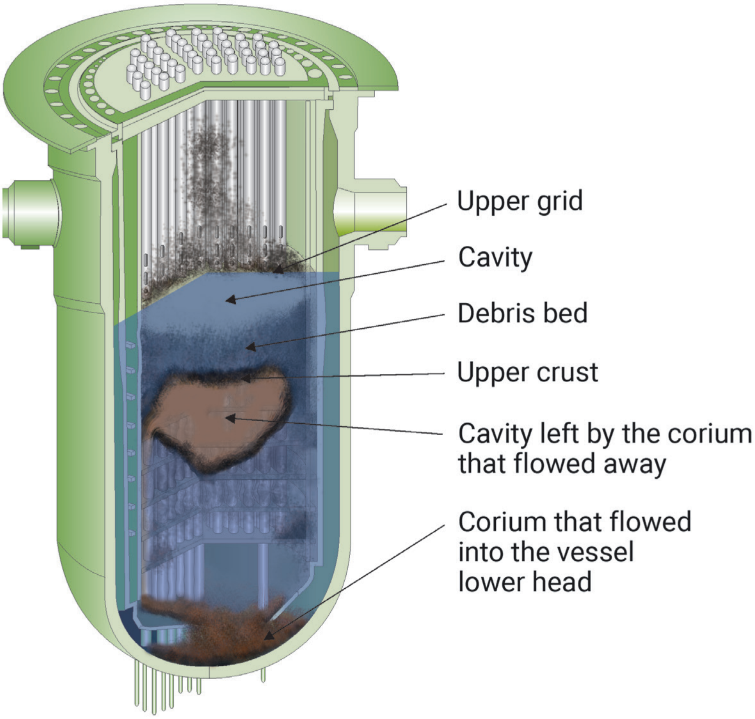

Upper grid
Cavity
Debris bed
Upper crust
Cavity left by the corium that flowed away
Corium that flowed into the vessel lower head

Figure 32.3. Final state of the TMI 2 reactor core. Georges Goué/IRSN.

Despite partial core melt and the subsequent significant release of radioactivity inside the reactor containment, the immediate radiological impact on the environment was minimal. The reactor building fulfilled its confinement function almost perfectly. Since the reactor containment had not been isolated from the rest of the facility, minor releases into the environment were caused by the transfer of contaminated liquid collected in the reactor sumps to an auxiliary building outside the containment.

Based on measurements of radioactivity levels taken at the site while the accident was in progress, it was estimated that, even though the auxiliary building in question had not been designed to be sealed like the reactor containment, only 0.01% of fission product inventory had been transferred from the core to the environment. As for iodine – bearing in mind that the isotope iodine-131 can have the most serious short-term impact if released into the environment – it was found that the total amount of iodine released to the environment was not more than 10^{-5} per cent of the inventory present in the reactor core (37×10^{10} Bq of iodine-131 were released in the 16 h that followed the beginning of the accident and approximately 259×10^{10} Bq were released over the next 30 days). Activity levels of other radioactive products released were estimated to include approximately 18.5×10^{9} Bq of caesium-137 and 3.7×10^{9} Bq of strontium-90.

A number of studies showed that the accident had no detectable impact on the health of either the public or workers at the plant and that it had no significant impact on the environment. In spite of this, people were terrified by the accident at Three Mile Island. For an entire week, the authorities in charge of protecting the population were unsure of how serious the accident was and debated whether or not to order the partial or total evacuation of local residents. They were especially concerned that the hydrogen bubble that formed in the upper section of the reactor vessel would explode (mistakenly since, with no oxygen in the vessel, an explosion was not possible), resulting in a disastrous loss of containment integrity and massive release of radioactive substances to the environment.

The contradictory nature of the information released by authorities as the emergency progressed did nothing to reassure the public, and over 200,000 people fled the region in the days following the onset of the accident.

During the accident, operating personnel at the plant received doses of a little over one millisievert, and had to wear protective face masks for a few hours. In the days after the accident, three workers received doses between 30 and 40 mSv while working together on coolant sampling operations.

The collective dose received by workers at the plant, from the moment that the accident was initiated to the time that fuel unloading operations ended in 1989, was an estimated 60 man-sieverts.

There were no deaths and no casualties.

32.3. Analysis of the accident causes

The data required to analyse the causes and consequences of the accident were very widely shared. All the parties concerned were able to make their own assessments, in the USA and in other countries. Many meetings were held and documents shared, leading to a broad consensus of opinion.

Nonetheless, the scale of the damage to the reactor core was underestimated by all those concerned until the vessel was opened and the degraded state of the reactor core could be observed.

The operators' misinterpretation of what was happening, their failure to understand the cause of the problems that they had had to deal with and the sequence of events – which led them to make a series of inappropriate choices – was highlighted. However, focusing on their mistakes does not explain the whole picture. In fact, the operators applied the procedures as required, but they did so based on incorrect or incomplete information. Analysis must focus more closely on why the operators failed to understand the sequence of events involved in the accident.

32.3.1. Error in identifying the position of the relief valve

The operators immediately checked the monitor in the control room indicating the position of the pressurizer relief valve and saw that it indicated that the valve was closed; but this information was wrong, since in fact it only indicated that the command to close the valve had been sent, rather than showing the actual position of the valve. This was one of the critical points in the accident sequence. The valve was not fitted with instrumentation designed to indicate its actual position because it is much simpler to obtain a signal in the control room indicating the electrical command sent from the control panel than it is to fit this valve, very difficult to access, with position sensors that are extremely difficult to adjust and service. There was nothing to inform the operators of this nonetheless essential difference.

The operators did, however, have several other means at their disposal to determine whether or not the relief valve was open or closed, including a readout of the temperature in the relief line leading out of the valve, and an indication of the water level in the pressurizer relief tank.

The operators did record the temperature of the relief line. It was abnormally high, but they did not think it was significant since they knew that the valve had been leaking quite badly for some time already. This line was therefore already at an abnormally high temperature during normal operating conditions on this reactor. The initial degraded state of the plant system meant that the operators had no means of diagnosing the failure of the relief valve.

The water level measured in the pressurizer relief tank was not monitored on the panel in the control room, but in an adjoining room. It seems that no one looked at this measurement because no instruction to do so was included in the operating procedure.

32.3.2. Understanding the behaviour of the pressurizer

Earlier it was mentioned that the operators were concerned by the rise in the liquid-steam interface in the pressurizer, which had reached and maintained a very high level, while pressure in the RCS was dropping.

It should be noted that, in all loss-of-coolant break situations except one, depressurization of the RCS occurs simultaneously with a drop in the water level inside the pressurizer. In this situation, the steam bubble at the top of the pressurizer pushes the water toward the break.

The one exception to this is the case where the break is located at the level of the steam bubble. Where this is the case, steam flows through the break, causing the water level in the pressurizer to rise, at least that is how it appears, thus lowering the pressure in the RCS.

This is what happened in the TMI accident, but the operators had not been trained to recognize or manage this specific situation. It was not covered in the accident management procedures. The operating crew was therefore unable to draw on either their training or any documentation providing a method for identifying and managing the situation. They were on their own, in uncharted territory.

But one point, which was not actually recognized until after the accident, was the fact that the pressurizer relief valve, used frequently, could become jammed in the open position, and this was not particularly uncommon for this type of reactor.

Eighteen months prior to the accident, the same scenario (pressurizer relief valve jammed in the open position) occurred at the Davis-Besse reactor, another US reactor of the same type. The operators had committed the same mistake in their analysis of the situation as at Three Mile Island (loss of cooling function) and failed to identify the fact that the valve was jammed for a full 20 min. However, the low decay heat of the fuel in this particular case avoided any impact on the fuel. According to the unwritten rule that says 'no impact, no problem', no one, neither the facility operator nor the analysts, even bothered to report this incident. Again, the workers had received no training and there was no applicable procedure.

The fact that this event was not recognized as a precursor to a severe accident highlights failures in how event feedback was managed. Yet another precursor event[887] had also occurred on 20 August 1974 at the Beznau nuclear power plant in Switzerland. During a sequence similar to that which had led to the TMI accident, a pressure-operated relief valve failed to close, causing the reactor to depressurize. In that case, however, the operators correctly identified the situation very quickly, within two or three minutes, and closed the isolation valve on the same line as the relief valve, thereby immediately stopping depressurization. Investigations did not specify what made the operators realize that the relief valve was open within such a short

[887] Pages 229 to 240 of M. Llory, *L'accident de la centrale nucléaire de Three Mile Island*, 1999, *Éditions L'Harmattan*, Paris.

time period. The reactor at Beznau was designed by Westinghouse and the event was analysed by a team employed by the designer, based in Brussels. Even so, the lessons learned from their analysis were not communicated to the American nuclear regulator, nor to Westinghouse's competitor, Babcock & Wilcox.

Last, it should be noted that the risks and the sequence of events involved in the TMI accident had been considered in engineering reports and reported in writing (including three letters sent by the Vinçotte association in 1971), but these reports were not adequately followed up.

32.3.3. Stopping safety injection

With the indicator showing that the water level in the pressurizer was rising and believing that the relief valve was closed, the operators manually stopped safety injection. The picture formed in the minds of the operators was false and they lacked direct information regarding the state of the reactor core and the reactor coolant system. There was nothing extraordinary about stopping safety injection – it was not uncommon for the safety injection system in Babcock & Wilcox pressurized water reactors to automatically start up under conditions in which it was not necessary. Nonetheless, this safety feature should not be stopped until a series of methodical checks based on predefined procedures has been carried out to assess the state of the RCS; but such procedures did not exist.

The operators also inhibited action of the safety injection system accumulators, which should have discharged automatically as soon as the pressure in the RCS fell below 45 bars. This is another example of their failure to understand what was happening.

32.3.4. Human-machine interface

The lack of information available in the control room and the associated faults have already been discussed briefly. But there were also other problems. Indicators showing the in-core temperature, restricted to a measuring range that was too narrow, appeared to be stuck at the high end of the scale. The operators thought this meant that the devices had failed. The control computer, overloaded with information, crashed and was down for two hours.

Before the accident, the reactor had been operating at nominal power. The emergency shutdown and the problems affecting the secondary side (failure of the steam generator emergency feedwater system) altered the state of many systems and parameters, which all triggered alarms. The control room itself has been described as being like a scene from a fairground, with a maze of lights lit up and flashing, and audible warning, alarm and alert signals all sounding at once. The emergency alarms were not arranged in any order that would have made it possible to distinguish initiating events from their normal consequences.

All these design faults in the human-machine interface combined to confuse the operators and prevent them from making an accurate analysis of the situation.

32.3.5. Isolating the reactor containment

In the design of the Three Mile Island plant, starting up the safety injection system did not automatically isolate the containment, in other words, it did not automatically close all valves on all pipes entering or exiting the reactor building and not essential for safeguarding the reactor core. The containment isolation function is designed to block exchanges between the inside and the outside of the containment, in order to minimize radioactive releases.

That is why the sump pumps were able to transfer water that was increasingly loaded with radioactive substances to an auxiliary building for several hours.

It was not until these transfers triggered radioactivity alarms in the auxiliary building that the isolation command was issued manually, hence quite late in the sequence of events.

This was a design error.

32.3.6. Confinement inside the auxiliary building

Water from the sumps entered the auxiliary building, but the pipes used and the storage tanks were not all leaktight, meaning that hot, contaminated water escaped into this building and then vaporized, releasing the iodine and xenon contained in the water.

These gases and vapours were drawn in by the building's general ventilation system and released to the outside environment through inefficient iodine filters. In fact, after the accident, it was found that these filters had not undergone the appropriate efficiency tests.

If the systems in this building had been tight and the iodine filters correctly inspected, these releases would not have occurred. Once again, conditions at the facility were degraded.

32.3.7. Emergency feedwater supply to the steam generators

Another failure state that exemplified the degraded conditions at the facility was the incorrect position of two essential valves in the steam generator emergency feedwater system. This time the fault was related to the quality of maintenance operations.

32.4. Lessons learned from the Three Mile Island accident

A great many lessons were learned from the accident at Three Mile Island which have since been taken into consideration to improve nuclear reactor safety. In France, from August 1979 and based on analyses carried out by IPSN, the Central Service for the Safety of Nuclear Installations (SCSIN) sent out a series of requests to Électricité de France (EDF) to improve safety in the French nuclear power plant fleet.

In spite of the in-depth scientific studies conducted in the USA on core-melt accidents in pressurized water reactors (as in the WASH reports mentioned above), it was only after the accident at Three Mile Island that nuclear facility designers and operators realized that such accidents really could happen.

Although the Three Mile Island accident did not call the underlying nuclear facility design[888] into question, it clearly demonstrated that accidents more severe than those considered until then in the design of nuclear power plants (such as a loss-of-coolant accident due to a sudden double-ended guillotine break in the reactor coolant system) are possible and may result from a sequence of technical failures and inappropriate actions.

The Three Mile Island accident raised many new questions, including the following:

- In responding to an accident situation, what can be done to prevent inappropriate operating actions from aggravating the consequences to the point of causing core melt?
- How can the reactor containment best be used as the last barrier capable of preventing the release of radioactive substances into the environment?
- Based on real-life incidents, what can be done to identify those incidents that could be precursors to a core-melt accident so that the necessary preventive measures can be taken in due time?
- How can nuclear facility operators and public authorities prepare to respond to a core-melt accident?

Reflection on these questions has focused on the human factor and its role in facility operations, feedback from nuclear facility operating experience and emergency response management.

32.4.1. The human factor in facility operation

Acknowledging the significance of human factors not only led to changes in organization, shared responsibility and recognition of the roles played by everyone involved, but also to technical changes.

a. Operating conditions must be improved

This implies more targeted action in the selection, initial training and continuous training of operators, including the systematic use of simulators as part of operator training. It was subsequently decided that full-scale control room operating simulators would gradually be installed at nuclear facilities. On this point, standardization of the French nuclear power plant fleet has made it easier for EDF to develop simulators that

[888] As described in Chapter 6, the fundamental safety principles, such as placing physical barriers between radioactive materials and the environment, required the implementation of measures to manage a certain number of accident scenarios, subsequently leading to the design of a robust confinement structure. It was primarily the containment that protected TMI facility personnel and nearby populations.

are directly representative of the different types of reactor used. Operator training must now cover not only normal operating conditions, but also incidents and accidents, giving operators the opportunity to experience a 'real-life' situation.

The Three Mile Island accident clearly demonstrated the inadequacy of the operating procedures available at the time. Operating instructions and procedures were reviewed and revised in most countries, particularly in France. This revision involved both the form (checking that the procedures were user-friendly) and the content of the documents.

As a result, a whole new approach to emergency response management has been deployed at facilities in order to:

– ensure, including in the event of an accident, 'human redundancy', with operators backed up by the Facility Safety and Radiological Protection Engineer, who was later to become the Facility Safety Engineer,

– ensure optimal management of the simultaneous occurrence of multiple, theoretically independent events.

Facility safety and radiological protection engineers are a specifically French idea, first proposed by Jean Bourgeois, the first director of IPSN. They are not called on to take direct action under normal operating conditions nor in the case of a 'conventional' accident. However, under abnormal conditions, they provide 'functional redundancy' by monitoring the situation from the Safety Parameter Display Console (described in more detail in point b). Changes to operating crews introduced as of 1993 retained more or less the same distribution of responsibilities with regard to safety; facility safety engineers, however, were no longer tasked with radiological protection nor were they members of the shift personnel any more, giving them greater independence in assessing the state of the facility.

Studies on scenarios involving the simultaneous occurrence of multiple events had been conducted in France since 1976, mainly drawing on the WASH-1400 report. Such scenarios were studied as 'beyond-design-basis'[889] events, and covered multiple-failure scenarios, including the loss of redundant systems. In the wake of the Three Mile Island accident, these studies led to the implementation – at all French nuclear power plants, which at the time consisted of 900 MWe reactors – of physical measures and operating procedures known as 'H' procedures ('H' for *hors dimensionnement*, meaning 'beyond-design basis'), intended to make core-melt prevention more robust (see Section 13.2).

Thereafter, from 1981 onward, the principle applied has been to implement 'U' procedures ('U' for ultimate) designed to prevent core degradation (U1) or, where this is not possible, to reduce release of radioactive substances outside the reactor containment to the minimum (U2 to U5). U procedures are designed to cover every type of situation regardless of the cause, unlike H procedures, as explained in Section 17.8.

A certain number of procedures (H procedures) have been tested using a simulator.

[889] Extending the range of 'conventional' situations that constitute the design basis; see Chapter 13.

b. Control room layout must be improved

As a result of findings from the Three Mile Island accident involving the lack of indications and prioritization of alarm displays in the control room, EDF made a number of changes to facility control rooms, including at facilities already in service. These changes focused on improving how information is presented – based on advice from trained experts in ergonomics and psychology – and replacing most of the 'command sent' indicators with indicators showing the actual position of the relevant devices. Certain measurement ranges were extended. New indications were added to provide more complete information on the state of the core (which was not available at the time of the Three Mile Island accident), such as the in-core subcooling margin (the difference between the actual temperature of the reactor coolant and its boiling temperature at the given pressure of the reactor coolant system) and the water level inside the vessel. In addition, alarms were prioritized and essential information was reproduced on the Safety Parameter Display Console, installed at one end of the main control panel in the control room.

The safety parameter display console consists of three sets of indications:

- status indicators, which indicate the state of safety systems and engineered safety systems as a result of the commands they have received: automatic reactor trip, safety injection, water spray inside the containment, containment isolation, etc.;
- the core-cooling monitoring system, which, based on pressure in the RCS and a certain number of temperature measurements taken inside the reactor vessel, monitors the in-core subcooling margin; the subcooling margin, often called Delta Tsat (ΔTsat), and the maximum reactor coolant temperature measured at the top of the fuel assemblies in the vessel are displayed on the safety parameter display console;
- a multi-function information system that collects, processes and displays information to provide diagnostic and control assistance.

The KIT/KPS system displays, in a synthesized and more detailed manner, the information that is also available to the operators in the control room; in particular, this includes the core-cooling monitoring system.

Two monitors and an interface panel, installed on the control console, are available to the operators. There is also a monitor and an interface panel, located at a distance from the main operating station but still in the control room, that can be used by the safety engineer to monitor the plant state without interfering with normal operations[890].

[890] A third station is located in the technical support centre where the engineers, gathered in the event of an emergency situation, can form an opinion on what is happening without disturbing the operating crew by asking for information. This is just one of the organizational measures implemented for emergency response management which will be covered in more detail in Chapter 38. It is interesting to note that the Remote Shutdown Station, designed to bring the reactor to hot and then cold shutdown, is only to be used if the control room must be evacuated, not in situations that also involve a different incident or accident; it is primarily intended to be used in the event of a fire in the control room.

These measures were deployed at all the reactors then in service (900 MWe units), and were subsequently included – with some minor differences – in the design of next-generation series up to and including the EPR.

Other lessons learned as a result of the Three Mile Island accident led to in-depth studies and changes to facilities, as follows.

c. Although fundamental nuclear power plant design principles remained unchallenged, many aspects could nonetheless be improved, such as:

- confinement functions provided by auxiliary buildings and ancillary systems;
- procedures for managing very large amounts of highly contaminated water and gases after an accident;
- valve quality and reliability; an important point to note here is that while safety valves are always designed to open, only nuclear facilities require that they also feature the ability to close and remain leaktight;
- the qualification of equipment for operation under accident conditions.

d. Safety assessment must not be limited to only assessing conventional operating conditions

Studies carried out in France since 1976 on multiple-failure situations were mentioned above. Nonetheless, it was only after the accident at Three Mile Island that the decision was taken to implement H procedures and the related physical protection measures at all French nuclear power plants, which at the time consisted of 900 MWe reactors.

32.4.2. Importance of precursor events

Another important lesson learned as a result of the Three Mile Island accident involves the use of feedback on nuclear power plant operating experience.

As mentioned earlier, a precursor incident very similar to the accident at Three Mile Island occurred in 1977 on the same kind of US reactor (Davis-Besse), but did not lead to reactor damage; the operators made the same error in their analysis of the situation as the crew at Three Mile Island. The lessons learned from that incident had not been incorporated into instructions available to operators before the accident occurred at Three Mile Island. The same can be said with regard to the event that occurred in 1974 at the Beznau nuclear power plant in Switzerland, where the operators managed to recover the situation. There too, neither the designers, Babcock & Wilcox, nor the US nuclear safety regulator were notified.

As these two examples illustrate, the systematic analysis of significant incidents and any changes to procedures available to operators that might be recommended as a result of such analysis, with a view to preventing any repetition of the same incidents, can be an effective means of preventing more severe accidents.

Since the Three Mile Island accident (and the studies that followed), the detection of precursor events likely to lead to an accident has become a major focus for facility operators and safety organizations. Follow-up of operations and managing operating experience feedback have therefore been developed with this objective in mind; the need to organize feedback within an international perspective has been recognized.

32.4.3. Study of complex situations and core-melt accidents, handling emergency situations

The accident at Three Mile Island also highlighted the fact that the operators, facility managers and authorities in charge of protecting the public were unprepared for dealing with a core-melt accident. The facility managers and the local and federal authorities did not know how the situation might evolve nor whether or not to evacuate residents. For about a week, authorities believed that a hydrogen explosion might occur, damaging the reactor vessel and the reactor containment and causing significant release of radioactive substances into the environment. This possibility could, in fact, have been eliminated early on, since the low concentration of oxygen in the core ruled out the possibility of a hydrogen explosion. Not knowing what to believe, many people living within a very wide radius of the facility left their homes, even though the authorities never announced the need to evacuate the area.

People in the industry realized that they needed to develop procedures for dealing with accident situations of this kind in a less random manner in the event that they might occur again, by:

– having greater confidence in the behaviour of the reactor containment, even under conditions much more extreme than the containment design-basis conditions,

– having tools designed to predict possible changes in the situation, the corresponding releases and their transfer to the environment under the given accident conditions.

More generally, the accident at the Three Mile Island nuclear power plant sparked a whole series of discussions, studies and research on situations that were more complex than the design-basis scenarios, such as accidents that could occur as a result of multiple failures, or core-melt accident situations, referred to as 'severe accidents'.

Complex accident situations eventually formed the 'complementary domain' of events, with research on these situations leading to the development and implementation of technical and organizational measures designed to manage these events and prevent them from degrading into a core-melt situation. The background behind the concept of the 'complementary domain' is described in Chapter 13.

Core-melt scenarios are described in greater detail in Chapter 17.

The Three Mile Island accident came about partly as a result of the operating crew's failure to understand what was happening due to design faults in the human-machine interface, partly due to the lack of appropriate procedures for dealing with the situation, and partly due to shortcomings in personnel training. It is not at all easy for any given operating crew to step back and question their initial interpretation of the situation. In addition to providing an independent opinion by introducing the facility safety and radiological protection engineers, it was thought that having an emergency response management team, distinct from the operating crew, and capable of analysing the situation from a broader perspective, might provide alternative points of view. Similarly, it appeared necessary to clarify the roles of the various entities involved and organize the dissemination of information in the event of an accident. Emergency response plans were developed on this basis. The need for regular training (emergency response exercises) was also emphasized.

Emergency response plans designed specifically for nuclear facilities were first developed in France in the early 1980s. On-site emergency plans were developed by nuclear facility operators with a view to optimizing accident management, mitigating the impact, providing on-site medical assistance and keeping public authorities informed.

Public authorities established off-site emergency plans to protect the population in the event of a severe accident at a nuclear facility.

On-site emergency plans and off-site emergency plans, together with more general information regarding emergency response management are described in greater detail in chapters 17 and 38.

32.5. Conclusions

A considerable number of lessons were learned from the accident at Three Mile Island, including the significance of defence in depth, the importance of human factors and operating procedures, together with how alarms are arranged and displayed for operators, and the crucial role of the containment as the ultimate barrier preventing release of radioactive substances to the environment. Reactors all over the world have benefited from the lessons learned as a result of this accident. Taking these lessons into consideration has improved safety at existing facilities.

Subsequent designs of new, third-generation reactors, especially the EPR, have also incorporated the lessons learned from the accident at Three Mile Island. Of particular interest, core-melt accidents have since been included in the design-basis scenarios for power reactors. For the EPR, in addition to the containment, designed to withstand any overpressure caused in different scenarios that could lead to core melt, a core-catcher at the bottom of the reactor containment serves to collect and cool any molten material that might begin to flow in the event of vessel failure.

Chapter 33

Incident and Accident Operation: from the Event-Oriented Approach to the State-Oriented Approach

As mentioned in Chapter 32, one of the lessons learned from the accident at the Three Mile Island nuclear power plant was that incident and accident operating procedures applicable at power reactors in the French fleet needed to be revised and improved. This entailed a considerable amount of work, which led to significant improvements in terms of safety. Nonetheless, it did not resolve all the problems related to the very principles on which procedures are based, which is the subject discussed in this chapter.

33.1. Limits of the event-oriented approach

Applying an 'event-oriented' approach meant that every incident and accident operating procedure (I or A procedure) was connected to a single initiating event as defined in the reactor design phase.

By extension, the complementary (beyond-design-basis) procedures, or H procedures, covered simultaneous multiple failures that were also clearly identified, since each scenario affected all the trains of a redundant system, and only those trains.

The aim of these procedures was to prevent, or at least mitigate, fuel rod cladding failure, the major potential source of any release of radioactive substances, and to restore the unit to a sustainable stable state.

It is interesting to compare what happened at Three Mile Island with the initiating events and combinations of initiating events used to develop I, A and H procedures. In the case of the Three Mile Island accident, the initiating event was a Category 3 operating condition (i.e. the pressurizer relief valve remained open, which is equivalent to a break at the top of the pressurizer), total loss of feedwater to the steam generators, even for a short period of time, and total loss of the safety injection system due the operators' failure to understand the situation.

As described in the previous chapter, reality can be extremely complex.

Event-oriented operating procedures cannot, therefore, cover all the possible combinations of events that might be involved in multiple, simultaneous or delayed equipment failures and human errors (such as an initial diagnostic error, incorrect application of a procedure, accumulation of incidents or accidents, total loss of an engineered safety system, etc.). Moreover, the greater the number of incident and accident sequences taken into consideration, the greater the number of procedures defined for managing each different scenario, making it practically impossible to assess the situation and choose the correct procedure – not to mention the fact that these procedures must be kept up to date, thereby making the document management system even more complicated.

The event-oriented approach also made it difficult, in terms of its practical application, to step back and reconsider the initial assessment of the situation if the development of events did not correspond to the events foreseen in the initial scenario.

To overcome these problems, Électricité de France (EDF) and Framatome, the nuclear steam supply system constructor, proposed an alternative approach to the choice of corrective measures to be applied in any kind of incident or accident situation: the state-oriented approach (SOA). In 1984, the Central Service for the Safety of Nuclear Installations (SCSIN) and IPSN launched discussions on this subject.

33.2. The State-Oriented Approach concept

The concept of the state-oriented approach is based on the realization that, while there may be a vast range of accident-initiating events and sequences, the number of possible states of reactivity, cooling and confinement that may characterize reactor operation is limited, whether under normal operating conditions or even the most degraded conditions.

This implies that it is possible to determine, for every abnormal state, an operating strategy and the action to be taken by the operators to bring the facility to a safe state. Based on continuous diagnostics of facility operation, the operating crew can take action without necessarily having understood the sequence of events leading to the incident or accident.

For this purpose, it was necessary to demonstrate that there is a direct relationship between observable states and the actions to be taken by the operators to improve the situation.

This required characterizing reactor reactivity states and the actions to be taken for each state. A similar amount of research was undertaken to characterize the thermal-hydraulics involved, in order to:

- identify all possible cooling states of the nuclear steam supply system, their domains of stability and the transients from one state to another,
- characterize these different states based on measurable physical parameters,
- determine, for each state identified, the most appropriate corrective actions or repairs to be performed by the operators – appropriate in the sense that they will improve the situation relative to the set of events that may have led to the state in question, without compromising the outcome,
- develop a system summarizing the points above which only differentiates between subgroups of states that require different actions,
- define the physical measurements and data processing required in the control room to perform diagnostics and monitor the effectiveness of the actions taken.

To characterize the thermal-hydraulics at work, nuclear steam supply system operation was therefore analysed in terms of the mass, energy and impulse balances for each main component in the system. It was then possible to characterize:

- the energy flow: produced by the fuel, removed by the reactor coolant, transported through the RCS and transferred out of the RCS,
- accumulation or release of energy in the reactor coolant and secondary systems,
- variations in mass of primary and secondary coolant.

For each of these characteristics, different configurations were defined, covering every possible physical combination, distinguished by measurable parameter values (pressure, level, temperature and their related time derivatives, void fraction in the RCS, radioactivity in the secondary lines of the steam generators, etc.).

All the possible combinations of these configurations were divided into groups, revealing that:

- the mass of reactor coolant, the circulation of coolant, and heat removal via the reactor coolant system determine the behaviour of the nuclear steam supply system and the heat removed from the fuel;
- heat removal from the reactor coolant system depends on the state of the secondary system and the possible presence of incondensable gases in the reactor coolant system, determined by what is known as the ‘pinch’, i.e. the difference between coolant temperature in the RCS and coolant temperature in the secondary system;
- the state of the secondary system in turn depends on the state of each of the steam generators, determined by the different masses of fluid in the secondary system, steam pressure and radioactivity levels in the secondary coolant.

Each overall state thus defined is linked to specific actions to be taken on the various systems, depending on their availability (safety injection, charging and letdown system, containment spray and pressurizer relief, emergency feedwater supply to the steam generators, discharge of steam from the secondary system, isolation of secondary feedwater and steam lines, etc.). These actions are selected with a view to stabilizing the state of the facility and, if possible, improve it by gradually passing into states of decreasing degradation.

In terms of practical application, the physical parameters characterizing the overall state of the facility were definitively classified according to six state functions:

- core subcriticality or nuclear power level,
- reactor coolant inventory,
- residual heat removal from the reactor coolant system,
- steam generator integrity,
- steam generator feedwater inventory,
- containment integrity.

To take into account the instrumentation available at the time when application of the state-oriented approach was first introduced – no measurement of the void fraction in the RCS, no indication of the water level in the vessel in 900 MWe units – states were grouped together without compromising the approach.

33.3. First application of the state-oriented approach

The first application of the state-oriented approach was the development of an ‘ultimate’ operating procedure, the U1 procedure, to be used in addition to the existing event-oriented procedures.

The U1 procedure was designed to ensure the best possible conditions for cooling the nuclear steam supply system and safeguarding the reactor core in situations where the I, A and H procedures, relating to clearly defined accident sequences, proved inappropriate or ineffective. The aim was, of course, to prevent or delay and mitigate damage to the reactor core and any resulting radiological consequences, depending on how severe the situation was and the means available to deal with it.

Depending on changes in core outlet temperature and the availability of systems and equipment, the U1 procedure indicated the best actions to be taken on:

- the steam generators,
- the safety injection system,
- the pressurizer relief valves,
- and the reactor coolant pumps,

to stop, delay or mitigate hazardous variations, thereby giving the operators time to restore the availability of failed systems.

The decision to abandon an event-oriented procedure in the course of its application in favour of the U1 procedure had to be made, following emergency shutdown, in the following cases (very simplified – see Figure 33.1):

- reactor core outlet temperature greater than 350°C,
- subcooling margin of the coolant (ΔTsat) less than 10°C combined with unavailable safety-injection system,
- no available steam generator (i.e. that could remove some of the decay heat without contaminating the steam),
- unfavourable change in the coolant pressure and temperature parameters,
- containment spray system unavailable combined with abnormal pressure, temperature and/or radioactivity level in the containment.

Rather than introducing these criteria into each event-oriented procedure, it was considered preferable to rely on continuous diagnostics:

- used according to an independent approach, in parallel to existing procedures, which therefore remained the same but could be changed separately in the future;
- by calling on the facility Safety Engineer, thus ensuring human redundancy with regard to the operators;
- supported by analysis of nuclear steam supply system cooling states and availability of engineered safety systems;
- using available instrumentation.

A specific Continuous Post-Incident Monitoring procedure was therefore established (referred to as SPI[891]). This was to be applied cyclically by the facility safety engineer, called to the control room as soon as an emergency reactor shutdown was triggered or as soon as the subcooling margin of the coolant fell below 20°C, and who remained on the scene until normal operating conditions were restored. Continuous monitoring covered the following parameters:

- the availability of each steam generator, i.e. its ability to remove part of the decay heat without contaminating the steam,
- the water mass in the reactor coolant system and the temperature of this water at the reactor core outlet,
- the ability of the secondary system to lower temperature and pressure in the reactor coolant system,

[891] *Surveillance Permanente Incidentelle*.

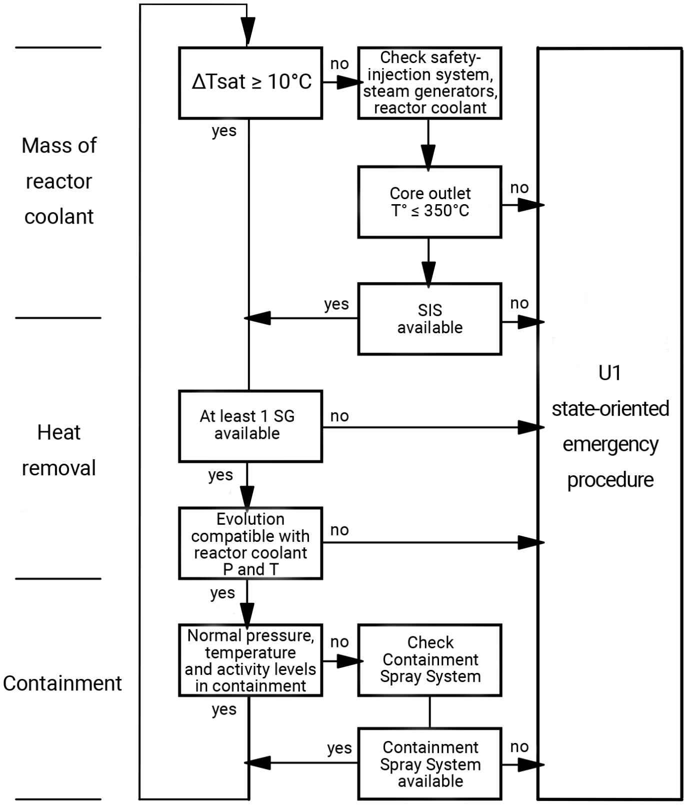

Mass of reactor coolant
Heat removal
Containment
ΔTsat ≥ 10°C
no
yes
Check safety-injection system, steam generators, reactor coolant
Core outlet T° ≤ 350°C
no
SIS available
yes
no
At least 1 SG available
no
yes
Evolution compatible with reactor coolant P and T
no
yes
Normal pressure, temperature and activity levels in containment
no
yes
Check Containment Spray System
Containment Spray System available
yes
no
U1 state-oriented emergency procedure

Figure 33.1. First application of the state-oriented approach: Continuous Post-Incident Monitoring (SPI) procedure and U1 procedure. IRSN.

- the effective startup of the engineered safety systems (emergency feedwater supply to the steam generators, high- and medium-head safety injection, low-head safety injection, containment spray system, etc.),
- pressure, temperature and radioactivity inside the containment,
- core criticality (neutron flux, position of control rods, boron concentration, etc.).

If necessary, the SPI procedure had to provide for the situation where the facility safety engineer chose to ask the operating crew to abandon the procedure (I, A or H) in progress and revert to the U1 procedure. The facility safety engineer would then continue monitoring by applying the Ultimate Continuous Monitoring procedure (referred to as SPU[892]) a new cyclic procedure for monitoring nuclear steam supply system performance in a declared site emergency situation.

[892] *Surveillance Permanente Ultime*.

Applying the SPI procedure usually confirmed, within a relatively short period of time, the main actions already required in the procedure applied by the operating crew. In some multiple failure situations, it required that operators perform additional limited actions such as isolating a steam generator, without abandoning the procedure in progress.

These new procedures (SPI, U1 and SPU) therefore formed a major addition to I, A and H procedures.

33.4. Widespread application of the state-oriented approach

Studies continued on the state-oriented approach and its precise and gradual implementation during frequent incidents. As a result, Penly and Golfech (1300 MWe reactors in the P'4 series) were the first nuclear power plants to integrate certain procedures based on the state-oriented approach when they were commissioned in 1990.

These procedures covered all types of thermal-hydraulic accident but did not apply to situations in which the reactor is connected to the residual heat removal system (RHRS). This set of procedures therefore covered, in progressive stages (but not in outage situations), all incident and accident situations affecting the reactor coolant system, from reactor trip to the most severely degraded situations, as well as secondary system operation, containment monitoring and the availability of certain systems. Therefore, there was no longer a break between the I, A and H procedures and the U1 procedure.

Other event-oriented procedures were available alongside these procedures for transitional purposes.

Responsibilities were shared between the operating crew and the safety engineer in the same way as before with regard to the conventional (event-oriented) operating procedures.

The state-oriented approach was then adopted more widely and was applied at newly commissioned N4 series units to control the reactor from the main control room, covering all reactor coolant system situations where the RCS is closed (connected to the RHRS or not), as well as loss of all systems important to safety. It was subsequently extended to states in which the RCS is not closed.

It was also gradually extended to the various 1300 MWe units, which were all equipped with instrumentation to measure the in-vessel water level, after retraining operators, taking into account feedback on experience gained from the earlier (N4) units, where the 'generalized' state-oriented approach had been applied.

This 'generalized' approach was then applied at 900 MWe units, from the late 1990s, once work had been carried out to install instrumentation for measuring the water level in the vessel.

33.5. 'Stabilized' state-oriented approach

After various 'generations' of the state-oriented approach, incident and accident operating procedures were stabilized as described below.

1. A document called the Diagnostics and Stabilization Document provided operators in the control room with guidelines on what action to take depending on the information and alarm signals received.
2. At the interface between normal operation and the state-oriented approach procedures, the operating crew now had a set of rules and procedures – including the Continuous State Monitoring procedure (SPE[893]), which replaced the Continuous Post-Incident Monitoring Procedure (SPI) – and incident operating procedures (the '**I-system**') which operators could be led to use in certain specific degraded situations:
    - in the event of a loss of main power supply, the islanding procedure,
    - in the event of loss of coolant or failure of RCS charging and letdown lines, the I-CVCS procedure (chemical and volume control system),
    - in the event of control rod malfunction, the I-CRDM procedure (control rod drive mechanism),
    - in the event of reactor coolant pump failure, the I-RCP procedure (problems specific to pump seals, for example),
    - in the event of problems affecting fuel assembly cooling or handling, the I-FPCPS procedure (fuel pool cooling and purification system) and I-FHS procedure (fuel handling system).
3. I, A and H procedures are integrated and covered by the **state-oriented approach**, which, depending on the state of the facility, proposes different strategies divided into four groups:
    - ECP (ECP1 to 4 in order of increasing severity): state-oriented operating procedures for the RCS and associated systems in reactor states where the RHRS is not connected,
    - ECPR (ECPR1 to 2 in order of increasing severity): state-oriented operating procedures for the RCS and associated systems in reactor states where the RHRS is connected and the RCS is closed,
    - ECPR0: state-oriented operating procedures for the RCS and associated systems in reactor states where the RHRS is connected and the RCS is open or not vented,
    - ECS: state-oriented operating procedure for the secondary side of the reactor.

[893] *Surveillance Permanente par États*.

In each group, there are several possible operating strategies: for example, the ECP[894] procedures include the strategies below:

- '*stabilization'* (return to normal operating conditions or wait in fallback state),
- '*soft shutdown'* (return to fallback state for repairs while approaching normal operating conditions: cooling at −14°C/h or −28°C/h),
- '*hard shutdown'* (rapid transition to fallback state with a hard cooling gradient of −56°C/h),
- '*stabilization/control of nuclear power'* (injecting boron to return the reactor core to a subcritical state and then adjusting boron concentration to reach a cold shutdown state),
- '*reduce ΔTsat'* (stabilize temperature and depressurize the RCS to prevent a cold shock to the reactor vessel and bring pressure and temperature within the standard state domain),
- *'restore residual heat removal'* (residual heat removal restored by switching to feed-and-bleed mode),
- '*restore reactor coolant inventory'* (re-establish water level at least in the hot legs, and then proceed to *'hard shutdown*'),
- '*ultimate core safeguard'* (to prevent or delay core melt by injecting water using any means possible).

Procedures and operations sheets are provided for each of these strategies.

In applying a state-oriented approach to operations, the operating crew monitors how the situation develops and, if necessary, can adjust the operating strategy as shown in Figure 33.2.

4. Last, to complete this set of procedures, beyond actual incident and accident operating procedures, and to cover more severely degraded states, the facility operator may still implement the four ultimate (U) procedures described in Section 17.8, referred to in the Assistance Guide for Emergency Response Teams and the Severe Accident Operating Guidelines:
   - U2: to locate and isolate leaks in the containment and reinject contaminated water into the reactor containment,
   - U3: to implement mobile emergency equipment for the containment spray system and the low-head safety injection system,
   - U4: to limit direct gaseous release (specifically in the case of the Cruas[895] nuclear power plant),
   - U5: to vent the containment via the sand-bed filter.

[894] See EDF Memento cited above and Section 8.2.1 of *Physique, fonctionnement et sûreté des REP* (Physics, Operation and Safety in Pressurized Water Reactors), B. Tarride, INSTN/EDP Sciences, 2013.

[895] See Section 17.5.8.

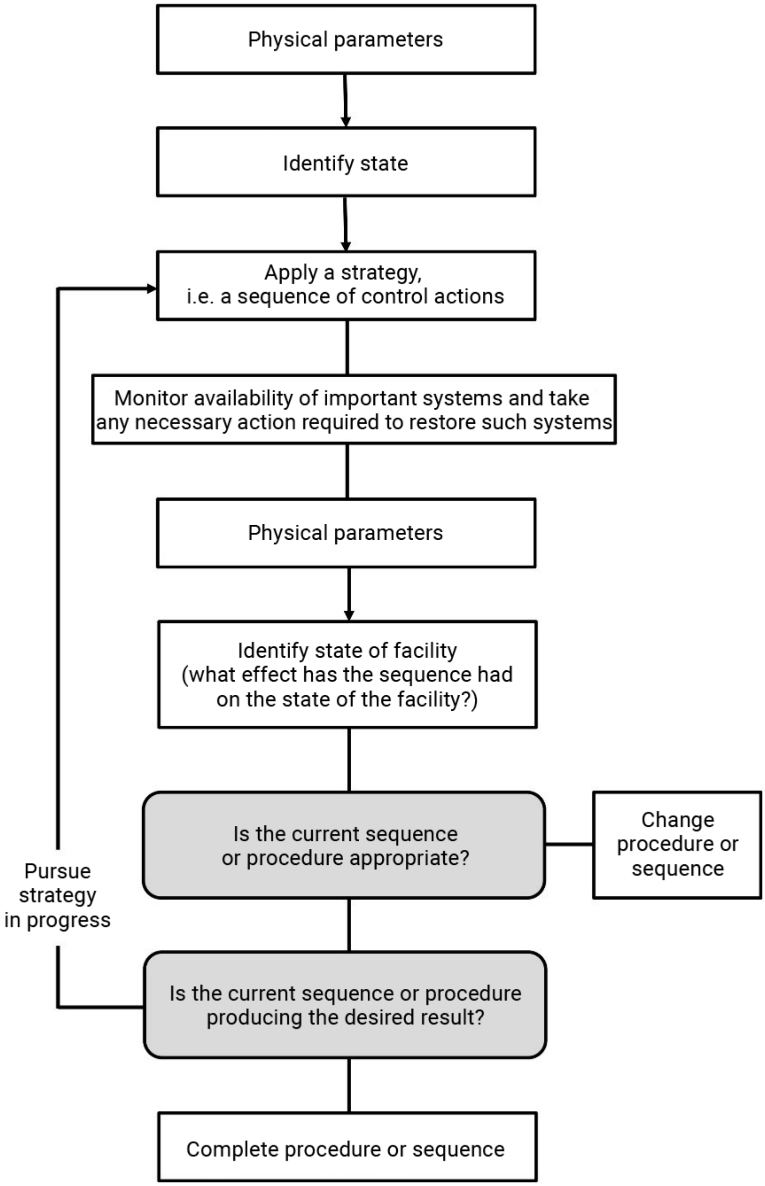

Physical parameters
Identify state
Apply a strategy,
i.e. a sequence of control actions
Monitor availability of important systems and take any necessary action required to restore such systems
Physical parameters
Identify state of facility
(what effect has the sequence had on the state of the facility?)
Is the current sequence or procedure appropriate?
Change procedure or sequence
Pursue strategy in progress
Is the current sequence or procedure producing the desired result?
Complete procedure or sequence

Figure 33.2. Cyclic flow diagram of the state-oriented approach. IRSN (source EDF).

33.6. State-oriented approach adopted for the EPR

For the Flamanville 3 EPR, the state-oriented approach has been adopted and applied in the design of incident and accident operating procedures. Operator guidance (Diagnostics and Stabilization, see above) is nonetheless automated.

Chapter 34
The Chernobyl Nuclear Power Plant Accident

On 26 April 1986, at 01:23:44 (local time), Unit 4 at the Chernobyl nuclear power plant in the former Soviet Union exploded. This is by far the most severe accident that has ever occurred at a civilian nuclear facility. It caused:

- two immediate fatalities due to multiple trauma;
- acute radiation exposure syndrome in 134 people, 28 of whom died within two months following the accident;
- the evacuation of 115,000 people in the days that followed the accident, followed by 230,000 more people in the period leading up to 1995;
- the irradiation and contamination of millions of people at levels which, while high, have proven difficult to assess accurately;
- since 1990, the onset of thyroid cancer in people contaminated when they were children living in the most severely affected regions in Ukraine, Belarus and Russia; several thousand cases of thyroid cancer have been identified, including about 15 fatalities;
- widespread deterioration in the health of members of the public who were exposed to the highest levels of radiation;
- the significant and long-term contamination of extensive areas of land in Ukraine, Belarus and Russia;

- major economic, social and psychological upset, as well as institutional and political upheaval in these same countries;
- measurable levels of contamination in many European countries, including France.

Between 1986 and 1987, over 300,000 people, known as 'liquidators', were involved in initial site clean-up operations, working in hazardous radiological protection conditions. More than 500,000 people were involved in clearing contaminated soils within a 30 km radius of the plant and in constructing the first sarcophagus.

The units at the Chernobyl nuclear power plant belonged to the RBMK[896] series. The design features of these reactors include the use of low-enriched uranium, graphite as the neutron moderator and cooling by boiling water circulating through pressure tubes. This type of reactor existed only in Russia, Ukraine and Lithuania, all of which were part of the former Soviet Union.

At the time of the accident, a test was being performed on the reactor under very specific conditions, outside its normal operating domain, at low power, and with some systems either unavailable or disabled.

Yet, as in the case of the Three Mile Island accident, it is necessary to look beyond RBMK reactor design and operator errors made during the reactor accident. While the accident was initially said to be caused by an accumulation of human errors, the focus gradually shifted, pointing to the need to develop:

- in-depth studies to define the minimal characteristics required for reliable safety organization in any country,
- the concept of 'safety culture',
- a more realistic and comprehensive approach to assessing possible releases resulting from an accident and their effects,
- awareness that reactivity accidents could occur at PWR facilities in the West,
- requirements to establish transparency in keeping the public informed.

In this chapter, the description of the accident sequence, analysis of the causes and the lessons learned draw mainly on the INSAG-7 report published in 1992[897], which includes two reports in the appendices: the first is the 1991 report by a commission to the USSR State Committee for the Supervision of Safety in Industry and Nuclear Power (SCSSINP), prepared at the request of the former USSR, and the second is the 1991 report established by a working group of USSR experts.

[896] *Reaktor Bolshoy Moshchnosti Kanalnyi,* or 'high-power channel reactor'.

[897] The Chernobyl Accident: Updating of INSAG-1, Safety Series No. 75-INSAG-7, 1992.

34.1. The Chernobyl nuclear power plant and RBMK reactors

The Chernobyl nuclear power plant is located in the extreme north of Ukraine, about a hundred kilometres north of Kiev, close to Pripyat, which was, at the time of the accident, a relatively new city developed to accommodate personnel from the plant and their families. The border with Belarus is only 10 to 15 km north of the facility, while the Russian border is 150 km to the northeast.

Unit 4 at the plant was one of fourteen 1000 MWe (3200 MWth) RBMK reactors in service at the time. Since the design of this type of reactor is quite different from Western reactors, a brief description is required (see Figure 34.1). The RBMK is a thermal neutron reactor with a graphite moderator, loaded with fuel elements made using uranium oxide enriched to 2% in uranium-235, contained in zirconium-niobium alloy cladding. The reactor has a very large graphite stack (11.8 m in diameter and 7 m high). The reactor is cooled by water which boils as it circulates from the bottom to the top of the pressure tubes (approximately 1700 in number), which are also made of zirconium-niobium alloy. The reactor unit is supported by a metal, welded structure contained in a concrete pit measuring 21.60 m on each side and 25.50 m in height.

Above the reactor, a refuelling machine is used to load and unload fuel from the pressure tubes while the reactor is operating.

Reactivity and output are controlled by 211 control rod assemblies housed inside pressure tubes identical to those described above, which are distributed across the entire core. These control rods are controlled by mechanisms installed above the core, and beneath the shielded floor of the reactor hall. They consist of rings of boron carbide, with a 4.5 m long graphite extension at the lower end.

The rod assemblies are inserted into and withdrawn from the reactor core by a motor-driven mechanism, at a maximum speed of 0.4 m/s. It therefore required 18 to 20 s to fully insert a control rod assembly from a fully withdrawn position.

The reactor is cooled by two separate primary coolant loops, each of which removes the heat produced from one half of the core. Each loop includes two water/steam separators (30 m long and 2.30 m in diameter) and four coolant recirculation pumps (three operating, one on standby). After passing through the reactor, a mixture of water and steam exits each pressure tube and is piped directly into one of the separators.

The water is then recirculated through 12 pipes to headers and recirculation pumps which feed water to the pressure tubes through a series of sub-headers and piping. There are 22 sub-headers, each measuring 300 mm in diameter, on each main coolant loop.

The coolant enters the reactor core at a temperature of 270°C, where it is heated up to a height of 2.50 m and boils at the top of the core. At the core outlet, the steam fraction at nominal power is 14.5%. Reactor outlet pressure is 70 bars and outlet temperature is 285°C. The flow rate in each pressure tube can be controlled by a valve to obtain satisfactory heat distribution.

Each loop feeds a 500 MWe turbine generator.

The graphite stack is only cooled by the pressure tubes. In operating conditions, core temperature is therefore high, except at the point of contact with the tubes in which the control rods are inserted and in the reflector.

There is an emergency cooling system for use in the event of a break in the main coolant system (pipe break on the coolant circulation line, break in a steam line or rupture in a feedwater supply line).

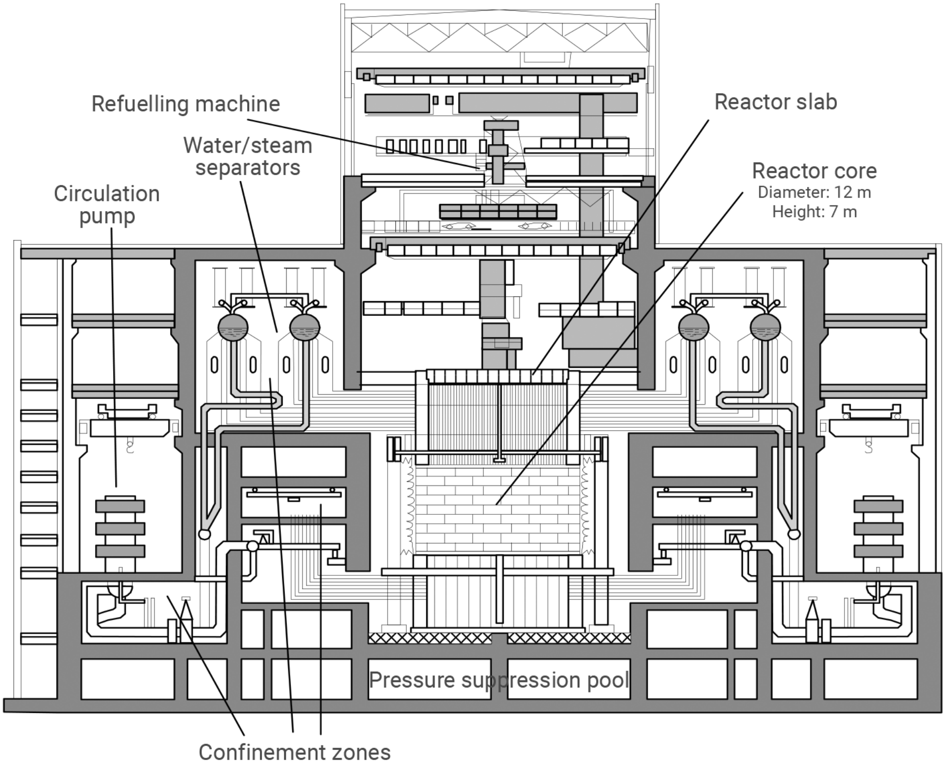


Figure 34.1. Simplified cross-section of a 1000 MWe RBMK unit. IRSN.

As in reactors designed in the West, the rupture scenarios used to define the characteristics of the emergency cooling system cover piping, headers and sub-headers, excluding larger capacity components such as the water/steam separators. It should also be remembered that, rather than a pressure vessel, the RBMK design uses a system of individual pressure tubes.

The design-basis accident involving engineered safety and confinement systems is the rupture of a 900 mm-diameter header, with loss of off-site power, taking into account a single failure mode. As for the core and the core coolant system, this choice is no different to that made in the case of Western pressurized water reactors.

However, confinement is based on a modular design, i.e. it consists of several sealed compartments designed to confine different zones in the event of a design-basis accident (in particular, a change in pressure due to a rupture). Four main zones are defined: the pipes that feed the pressure tubes, the main coolant system pipes and pumps, the steam lines and the reactor core itself.

The modules are directly or indirectly connected to the pressure suppression pools, which are designed to condense steam from any pipe breaks, and are located under the pit that contains the reactor core.

According to the Soviet designers, the advantages of this type of reactor are the absence of a pressure vessel, the absence of steam generators, the ability to continuously renew the fuel, thereby providing fuel-cycle flexibility, and the ability to adjust the coolant flow rate in each channel.

The disadvantages of such a reactor include the complexity of the coolant distribution and collection system, the intense accumulation of thermal energy in the metal structures, graphite stack and the fuel and, most importantly, the difficulty and complexity of managing and adjusting the power level and power distribution.

This last point merits further explanation. As noted above, the core of a 1000 MWe RBMK reactor is extremely large: 11.8 m in diameter and 7 m in height. Radial and azimuthal power oscillations due to the ‘xenon effect’ are very easily produced in a core of this size. Controlling these oscillations requires a large number of sensors and extensive use of the control rod assemblies. Given the sensitivity of in-core sensors, a fine reading of core power distribution can only be determined when operating 10% above nominal power; below that, operators only have general information on the state of the reactor provided by sensors located outside the core on the median plane.

In addition, the quantity of graphite as compared with the quantity of fuel, and their respective layouts, largely ensures that neutrons are slowed down. Under these conditions, if there is low neutron absorption in the core (few control rods inserted, low uranium-235 content in the fuel due to low initial enrichment or to fuel burnup), the coolant no longer acts as a moderator, unlike what happens in pressurized water reactors like those in the French power reactor fleet, which are intentionally undermoderated. This implies that the water is predominantly acting as a neutron absorber.

Any rise in temperature reduces coolant density, thereby reducing overall absorption of neutrons in the core. This effect increases when part of this water boils at 70 bars, representing a reduction in density by a factor of 20, increasing the proportion of neutrons available to cause fission reactions. Reactor power will then tend to increase, thereby amplifying this phenomenon.

The power coefficient in relation to coolant temperature is therefore positive within part of the operating domain. The power coefficient in relation to the vaporization rate (generally known as the void fraction) is also positive since it consists of the same phenomenon.

Fortunately, this is not the only effect at work and the neutron effect of a rise in fuel temperature is always negative due to the Doppler effect, the absolute value of which increases with temperature.

The total power coefficient, which is the sum of the two effects mentioned above plus some other less significant effects, is negative at high power, but positive at thermal power of less than 700 MW. Moreover, this coefficient becomes more positive the more control rods are withdrawn from the core.

It is interesting to note that in RBMK reactors, when the control rods are very high, their insertion begins by displacing water and replacing it with graphite in zones where neutron flux is high, thus injecting reactivity instead of removing it. This effect was observed as early as 1983 at the Ignalina plant but, although it was notified as a potential hazard to other sites where RBMK units were in operation, including at Chernobyl, no modifications or measures restricting operation were adopted and the issue was forgotten.

Regarding the thermal-hydraulic conditions, it is important to note that a given increase in power produces proportionately more steam when the initial power is low, the mass flow rate of the coolant being almost proportional to power.

These physical data should have been covered by two strict safety restrictions in RBMK operating documents:

– the reactor must not operate continuously below 700 MWth; this constraint was not stated explicitly in the operating procedures;

– in normal operating conditions, the equivalent of 30 control rods must be inserted in the core. The second measure, which was stipulated in the operating procedures, was considered as necessary for controlling power distribution rather than being essential for ensuring facility safety. Inserting the equivalent of 30 rods also reduced the effect of positive reactivity produced by insertion of the graphite ends when other rods were inserted.

The equivalent number of rods that must be inserted in the core was associated with the concept of the Operating Reactivity Margin (ORM) which, as observed in INSAG-7, was not very precise and was poorly understood by the operators.

In addition, the information available to operators in the operating procedures stated that:

– during steady-state operation, the operating reactivity margin was not to be less than the equivalent of 26 to 30 inserted control rods;

– reactor operation with an equivalent of less than 26 inserted control rods required authorization from the facility manager,

– at an equivalent of 15 inserted control rods or less, the reactor was to be shut down immediately.

RBMK units were equipped with an ORM calculator; however, this calculator did not have the capacity to provide real-time information, especially during rapid transients, the computing cycle requiring several minutes (10 to 15 min according to the INSAG reports, 5 min according to Soviet reports). In addition, the information was only accessible in a room located 50 m away from the control station.

34.2. The accident sequence

It is important to remember, before reading on, that in the sequence of events described in the Soviet reports and the INSAG-7 report, the ORM values given, expressed as an equivalent in total number of control rods inserted in the core, are based on computer modelling performed after the event. In any case, while the test was being conducted, it seems that no one checked the data provided by the ORM calculator which, given the time required to calculate the ORM, may have displayed information relevant to a state that had been reached several minutes earlier.

Chernobyl Unit 4 had been in service since December 1983. A reactor outage was scheduled for 25 April 1986 to carry out maintenance work that could not be performed during operation. A specific test was also scheduled to be performed just before unit shutdown, to check whether, in the event of a loss of off-site power, it was possible for one of the turbine generators to supply enough electrical power while it was slowing down under its own inertia, for a few tens of seconds, long enough to keep the main reactor coolant recirculation pumps in operation until the emergency diesel generators took over[898]. This type of test had already been performed for Unit 4, but had been disturbed by electrical problems. A new voltage control system had been installed. The test was supposed to be performed starting from a thermal power of 700 to 1000 MW.

Power reduction started on 25 April. At about 13:00, the reactor was operating at 1600 MWth, i.e. at half power. At that point, decoupling of one of the turbine generators occurred. In compliance with the test programme, the emergency core cooling system (ECCS) was isolated, although the reasons for this isolation were not very clear.

At that point, the off-site electrical load dispatcher requested that the power drop be stopped in order to continue to supply the power grid with 500 MWe. The reactor therefore continued to operate at half power for 9 h. While this plateau was maintained, xenon poisoning of the core had enough time to increase to its maximum value at 500 MWe. To compensate for this effect, some control rods were gradually withdrawn. In the meantime, no one had restarted the emergency core cooling system, since extended operation with an inhibited safety system was not considered to be hazardous.

[898] This test was meant to be performed during startup tests, but had not been conducted at Unit 4 of the Chernobyl plant. It had been carried out on other reactors, between 1982 and 1986, without any reported incidents.

At about 23:00, power reduction resumed. An hour and a half later, when switching from the automatic power control system to the manual system, something went wrong. Power dropped to 30 MWth. Automatic control was therefore lost. Xenon poisoning in the core started to increase again. Very little steam was being produced in the core. This required removing even more control rods to raise power slightly, which stabilized at 200 MWth on 26 April at about 1:00 in the morning.

The reactor was therefore no longer operating within the steady-state domain required in terms of the operating reactivity margin (with power below 700 MWth – the ORM was, at that moment, less than the equivalent of 30 inserted control rods). The operating crew decided to proceed with the scheduled test, according to the initial test programme.

Two additional reactor coolant circulation pumps were started up at 01:03 and 01:07, causing a sharp increase in the coolant flow rate in the core, above authorized values. This lowered core power to a level below that expected when preparing the test, making it difficult to maintain steam pressure and the water level in the separators within their normal ranges. The crew then disabled the emergency reactor shutdown signals associated with these parameters, according to the test programme.

At 01:22, given the accumulation of xenon, and according to calculations made after the accident, there was only the equivalent of 6 to 8 control rods inserted in the core, even though an immediate shutdown was required when there was only the equivalent of 15 inserted control rods. Whatever the reasons, the reactor was not shut down immediately. The crew decided to conduct the test and, in order to be able to repeat the test if necessary, disabled the emergency shutdown signal associated with shutdown of the second turbine generator.

At 01:23, the steam inlet valves on the turbine were closed, but the reactor was not shut down. The circulation pumps powered by the turbine generator slowed down, the flow rate decreased and the coolant heated up and vaporized. The void effect caused a release of reactivity. Power increased in the core, creating even more steam. The situation became divergent.

At 01:23:40, the shift supervisor gave the manual command for immediate insertion of the control rods, but this did not have the desired effect, quite the opposite in fact. The parts of the control rods lowered into the core were the graphite displacer ends, which, displacing the water that was in the pressure tubes, caused a considerable rise in reactivity in the core. Inserting the control rods actually boosted the increasing void fraction, causing a power excursion!

According to various post-accident calculations, instantaneous reactor power reached possibly 100, or even up to 500 times its nominal power within a matter of seconds. The chain reaction was stopped by negative reactivity produced due to the increased temperature of the fuel (Doppler effect) and due to destruction of the core.

The description of what happened next is based on visual observations, off-site radiation measurements, existing knowledge of fuel behaviour during reactivity accidents, post-accident calculations and postulated scenarios. It is still difficult to confirm categorically that the scenario presented below is what actually happened, particularly with regard to the order in which certain phenomena may have occurred.

The power excursion generated significant energy deposition in the fuel pellets, which fragmented into very fine particles; uranium oxide was released in the form of powder dispersed through the channels. Water in the core then interacted with very hot dispersed fuel particles, leading to massive vaporization, increasing pressure and probably causing a steam explosion (these phenomena are described in Chapter 17). The resulting explosion ruptured some of the pressure tubes, raising the upper slab (weighing 2000 tonnes) of the reactor, ripping out the other channels and horizontal steam lines leading to the headers, taking the control rods with it. The energy released by the explosion was estimated to be equivalent to the explosion of 30 to 40 tonnes of TNT.

A second explosion occurred almost immediately after the first. It may have been due to a deflagration of the hydrogen released by a reaction between the water and the zirconium in the pressure tube cladding and mixed with air after the reactor core was blown open. It may also have been caused by the effect of reactivity due to generalized boiling of the water which went from 70 bars to atmospheric pressure when the pressure tubes failed.

The reactor superstructures were destroyed.

The explosion caused incandescent debris to shoot out from the reactor core, which was exposed to the air, sparking thirty outbreaks of fire in Unit 4 and in the adjoining unit. The plant emergency teams and fire-fighters from Pripyat and Chernobyl (about 15 km from the facility) responded very quickly and extinguished all the fires in less than three and a half hours. They did not have adequate protective equipment to shield them from contamination or burns, the effects of which added to the effects of external exposure; 28 of the responders died in the days following the accident, in addition to the two people who were standing on top of the reactor's upper slab and were killed immediately as a result of burns and multiple trauma at the time of the accident.

Water was rapidly injected into the damaged core in an attempt to cool it and prevent the graphite from catching fire, but this proved unsuccessful.

Post-accident examinations suggest that very high temperatures (at least 2600°C) were reached in the reactor core and that part of the core melted. Over the six days following the explosion, these molten materials flowed to the bottom of the core and accumulated beneath it, forming a crucible-shaped crust above the concrete slab below. This stable, thermally-insulating crust resisted for four days, finally breaking apart about ten days after the explosion, allowing the molten materials to flow down onto the concrete slab below. The molten materials then cooled and solidified, thereby reducing the emission of radioactive substances. The concrete base slab, 1.8 m thick, was penetrated to a depth of 1 m by the molten materials.

On top of all this, at 5:00 (i.e. about three and a half hours after the explosion), the graphite ignited. It is possible that rising temperatures in the cold parts of the graphite stack caused a Wigner Effect[899], contributing to the release of energy and promoting ignition of the graphite. Many of the fire-fighters received excessively high doses of radiation in their attempts to suppress the fire. The enormous stack of graphite burned for about ten days and it is more than likely that, following the explosion, this fire was what caused the dispersion of radioactive substances into the atmosphere at high altitudes, leading to the contamination of a large part of Europe.

Helicopters were used to drop a combination of materials – sand, boron, clay, dolomite, and lead – on top of the reactor to try to stop the fire and confine releases of radioactive substances. Between 27 April and 2 May, 5000 tonnes of materials were dropped on top of the reactor to gradually cover it, in an attempt to reduce air flow to the graphite and thereby the release of fission products. In spite of these efforts, significant releases continued from 26 April to 5 May 1986. Releases continued thereafter for about another twenty days, but at much lower levels once the graphite fire had been extinguished and the molten materials had been cooled and partially solidified.

From 5 May, pressurized nitrogen was injected beneath the reactor to cool the molten materials and the concrete of the slab below. A heat exchanger was then placed in this part of the unit. This helped cool and solidify the molten materials.

Figure 34.2 shows damaged Unit 4 at the Chernobyl nuclear power plant.

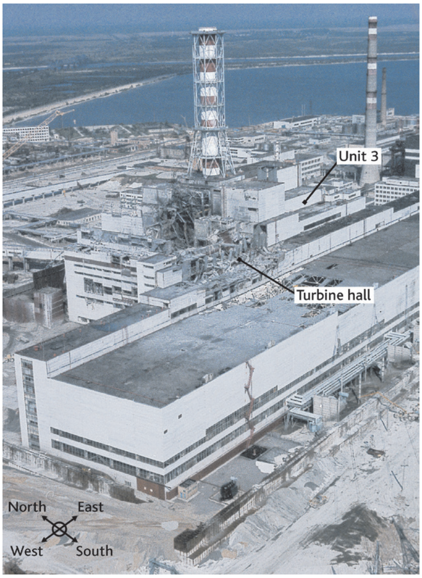


Figure 34.2. Unit 4 at the Chernobyl nuclear power plant following the accident.

[899] Neutron irradiation of graphite damages the crystal lattice of the graphite. This damage is exacerbated if the temperature of the graphite is less than 350°C. These faults each store a certain amount of energy. If the graphite temperature rises above 350°C, the stable form of the crystal lattice is restored, immediately releasing the energy stored within. This is the phenomenon that occurred in 1952 at the Windscale reactor in the United Kingdom.

In the months following the accident, work was carried out to isolate the damaged unit beneath a massive concrete structure. The particularly difficult construction conditions resulted in a 'sarcophagus' that did not ensure confinement for a very long time. In 1995, work was carried out to reduce the amount of water penetrating through the sarcophagus, until more extensive work could be carried out.

In 1997, the Shelter Implementation Plan (SIP) was launched to transform the site into an 'ecologically safe' zone. The main objectives of this plan were:

- Stage 1: to stabilize the engineering structures of the existing sarcophagus.
- Stage 2: to construct a new 'safe containment'.
- Stage 3: to dismantle the existing sarcophagus and remove the radioactive materials contained inside it.

The first stage of the plan was completed in 2008.

In September 2007, a contract[900] was signed for the construction of a new containment structure designed to completely enclose the old sarcophagus. The new, arch-shaped containment consists of a gigantic metal framework weighing over 18,000 t, 162 m long, 108 m high, with a crosswise span of approximately 257 m (Figure 34.3).

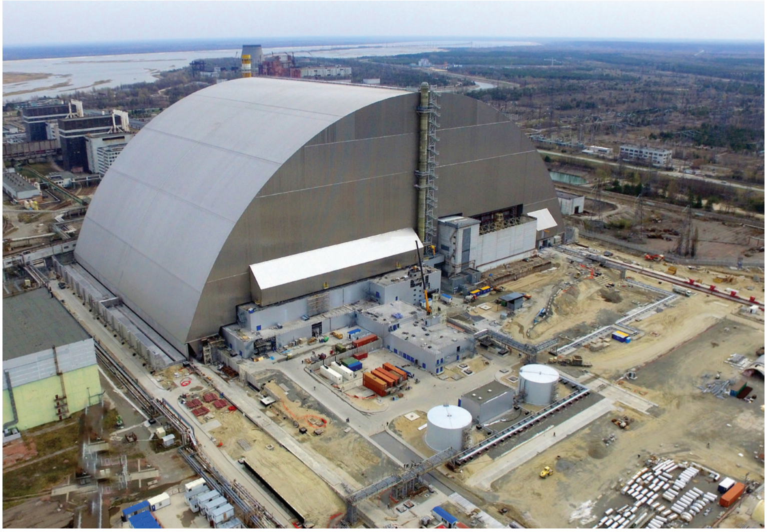


Figure 34.3. The new sarcophagus after installation – photograph taken in 2017. EBRD.

Before work could begin on building the new sarcophagus, 55,000 m^3 of contaminated materials were removed and a 30 cm-thick concrete cover was poured to ensure the safest possible working conditions for the 10,000 people involved in constructing the New Safe Containment.

[900] The plan was mainly funded by the European Union and the European Bank for Reconstruction and Development (EBRD).

Work to install the new sarcophagus was finally completed at the end of November 2016 (see Figure 34.3). It now completely encloses Unit 4 of the Chernobyl nuclear power plant. Work nonetheless continues inside to ensure that the new sarcophagus is completely sealed (particularly by connecting it to the first sarcophagus by means of a membrane) and to prepare for removal of debris remaining beneath the first sarcophagus.

34.3. Analysis of the accident causes and changes made to RBMK units soon after the accident

Initial reports made by the Russian authorities put all the blame for the accident on the operators, emphasizing the ways in which operating procedures had been violated. It later appeared (see the INSAG-7 report) that such procedures did not exist or were neither clear nor understood, and that the real causes of the disaster were the reactor design, the lack of safety studies, inadequacy of the operating rules and documentation and the ensuing level of training, as well as inadequate inspection by safety regulators. This incriminated the entire Soviet nuclear industry, including designers, constructors, facility operators and safety organizations.

It seems that when the test programme was being prepared, the impact of this programme on safety issues was not taken into consideration. The test programme did, however, call for some major departures from the operating rules, such as stopping the safety injection system and starting the eight coolant recirculation pumps, which implied a clear reduction in the level of safety. The facility safety team did not review the test programme and it should have been supervised by an electrical engineer.

During the test, a number of automatic safety systems were disabled, namely:

- safety injection,
- the emergency reactor shutdown function triggered by level or pressure alarms from the separators,
- the emergency reactor shutdown function triggered if the second turbine generator stops functioning.

In addition, the operating crew pursued operations even though the unit was operating outside the limits given more or less clearly in the operating procedures. In particular, this included:

- operating without safety injection for 9 h,
- prolonged operation at a power level below 700 MWth,
- an operational reactivity margin well below the required equivalent of 30 inserted control rods, and even below the equivalent of 15 inserted rods,
- pursuing operations in spite of the immediate shutdown procedure that should have been applied in response to the low number of inserted rods.

The operators acted as though they had no idea of the possible consequences of failing to comply with these operating conditions.

Apparently, such practices were not uncommon. They must therefore have been known and tolerated by facility management and by the resident inspectors of the safety regulator.

These operating errors were compounded by errors in the design of this type of reactor, including:

- core instability at low power, due to the positive void coefficient created by the coolant;
- the absence of a fast and effective reactor shutdown system that has no immediate adverse effects;
- the lack of automated protective features combined with many opportunities to inhibit safety features. A much greater level of reliance was placed on the operators than on automated systems, considered, at the time of early reactor design, to be less reliable.

Very soon[901] after the accident, various measures were identified by the designers to make RBMK reactors less vulnerable to errors and non-compliance with operating procedures.

Uranium enrichment was increased from 2% to 2.4% and the number of control rod assemblies in the core was raised (by an additional 30 to begin with, raised to 80 at a later stage), thereby increasing neutron absorption in the core and reducing positive reactivity effects.

All control rods were fitted with a device ensuring a minimum insertion of 1.20 m in the core, and now 70 to 80 rods must remain inserted in the core. These two measures reduce the positive void coefficient and place the rods in an immediately effective position. The time taken to insert the rods was also reduced from 19 to 2.5 s. Lastly, they were modified to eliminate the positive reactivity effect at the beginning of insertion.

The operating reactivity margin was strictly defined as the equivalent of 43 to 48 inserted rods, depending on the reactor, rather than the equivalent of 30 or 15 rods required before the accident. The computer program used to calculate the ORM was changed to ensure that this information is reported to the control room.

Changes were also made to the depressurization system to enhance its residual heat removal capacity.

[901] The INSAG-7 report and the Soviet reports highlight the fact that, well before the Chernobyl accident, although the designers were well aware of the risks inherent to the specific features of RBMK reactors, this had not resulted in any substantial changes or restrictions in operating procedures.

34.4. The other units at the facility

The other units at the Chernobyl site have now all been shut down and construction of units 5 and 6, begun in 1981, has been abandoned.

Spent fuel has been unloaded from units 1, 2 and 3, and is now in a storage pool built at the site. A dry spent fuel storage facility has also been built at the site, where cooling is ensured by air circulation. Once all the spent fuel has been transferred to this facility, the storage pool will no longer be required.

34.5. Radioactive release and protection of the population

The most recent official report on the radioactive release and health effects resulting from the Chernobyl accident is to be found in the UNSCEAR (United Nations Scientific Committee on the Effects of Atomic Radiation) report presented to the General Assembly of the United Nations in 2008, and more particularly in its Scientific Annex D[902]. This report was preceded, in 2006, by a report from the World Health Organization[903] (WHO), and an IAEA[904] report. The following discussion is based on information from all these texts and also on more recent data, including that published in 2018 by the UNSCEAR, which provides up-to-date information on the incidence of thyroid cancer in regions affected by the Chernobyl accident[905].

34.5.1. Radioactive release kinetics

One third of the radioactive release occurred immediately, at the time of the explosions when the reactor was blown open (Figure 34.4); the other two-thirds, released between 27 April and 5 May, consisted of variable mixtures of radionuclides, depending on temperature in the various zones of the fuel, but all contained iodine and caesium and, most probably, noble gases, in varying proportions depending on the phase.

As the reactor core was gradually covered with materials dropped by helicopters, from 2 May, temperature in the core began to rise, since the effect of core cooling was diminishing, causing an increase in radioactive release until 6 May when the graphite fire was finally extinguished and molten material cooled and partially solidified.

[902] UNSCEAR 2008 Report to the General Assembly with Scientific Annexes, entitled Sources and Effects of Ionizing Radiation, available at: http://www.unscear.org/docs/reports/2008/11-80076_Report_2008_Annex_D.pdf.

[903] Health Effects of the Chernobyl Accident and Special Health Care Programmes. Report from the UN Chernobyl Forum Expert Group – Geneva, 2006, available at: http://www.who.int/entity/ionizing_radiation/chernobyl/en/index.html.

[904] Environmental Consequences of the Chernobyl Accident and their Remediation: Twenty Years of Experience. Report from the Chernobyl Forum 'Environment' Expert Group, IAEA, 2006.

[905] UNSCEAR report entitled Evaluation of Data on Thyroid Cancer in Regions Affected by the Chernobyl Accident, 2018.

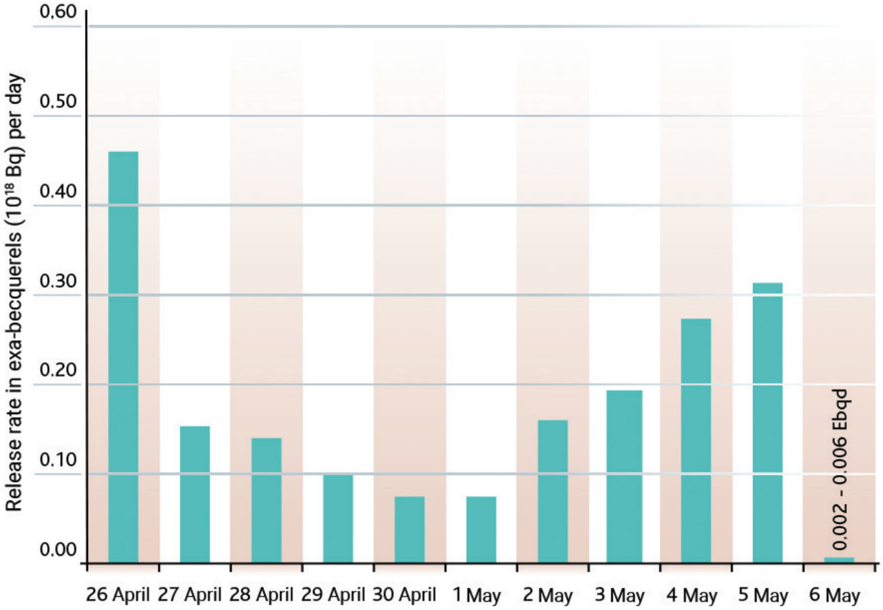


Figure 34.4. Daily release rate of radioactive substances to the atmosphere, excluding noble gases, after Unit 4 of the Chernobyl nuclear power plant exploded, IRSN (source: IAEA, 2006 see Footnote 904).

Table 34.1. Estimated activity of the main radionuclides released in the course of the Chernobyl accident (source: IAEA, 2006).

Element	Radionuclide	Symbol	Radioactive half-life	Total activity released in PBq (10^{15} Bq)
Inert gases	Krypton-85	^{85}Kr	10.7 years	33
	Xenon-133	^{133}Xe	5.3 days	6500
High-volatility elements	Iodine-131	^{131}I	8 days	~1760[906]
	Iodine-133	^{133}I	20.8 hours	2500
	Caesium-134	^{134}Cs	2.1 years	~47
	Caesium-136	^{136}Cs	13.1 days	36
	Caesium-137	^{137}Cs	30.2 years	~85[907]
	Tellurium-132	^{132}Te	78 hours	~1150
Low-volatility elements	Ruthenium-103	^{103}Ru	39.3 days	> 168
	Ruthenium-106	^{106}Ru	1 year	> 73
	Strontium-89	^{89}Sr	50.5 days	~115
	Strontium-90	^{90}Sr	29.1 years	~10
	Barium-140	^{140}Ba	12.7 days	240

[906] i.e. 50 to 60% of iodine-131 activity contained in fuel in the core.

[907] i.e. 20 to 40% of caesium-137 activity contained in fuel in the core.

Element	Radionuclide	Symbol	Radioactive half-life	Total activity released in PBq (10^{15} Bq)
Refractory elements (non-volatile)	Zirconium-95	^{95}Zr	64 days	84
	Cerium-141	^{141}Ce	33 days	84
	Cerium-144	^{144}Ce	285 days	~50
	Neptunium-239	^{239}Np	2.4 days	400
	Plutonium-238 -239 -240	Pu	87.8, 2.41 x 10^4 and 6563 years, respectively	< 0.1
	Plutonium-241	^{241}Pu	14.4 years	~2.6
	Curium-242	^{242}Cm	163 days	~0.4

Radiation release from these radionuclides was therefore commensurate with source term S1 release (see Chapter 17).

The reactor explosion, the extremely high fuel temperature, and the graphite fire that lasted for about ten days, caused dispersion of gases, aerosols and particles at high altitude, which somewhat attenuated consequences in the immediate vicinity but facilitated radionuclide dispersion across Europe.

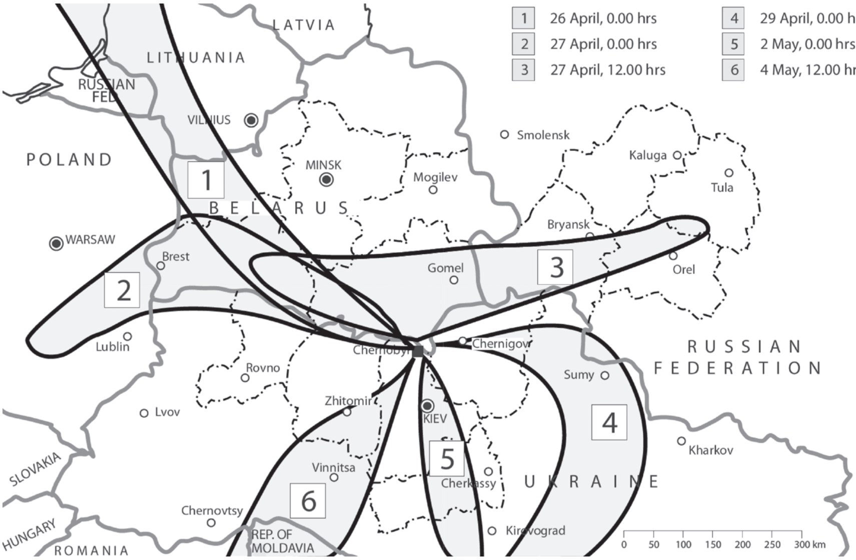


Figure 34.5. Release pathways, from 26 April to 4 May 1986 (image from V. A. Borzilov and N. V. Klepikova, Effect of Meteorological Conditions and Release Composition on Radionuclide Deposition After the Chernobyl Accident, in S. E. Merwin and M. I. Balonov (dir.), The Chernobyl Papers. Doses to the Soviet Population and Early Health Effects Studies, Volume I, Washington, Research Enterprises Inc., p. 47-68, 1993).

Extremely variable weather conditions dispersed radionuclides in nearly every direction (see Figure 34.5). When the radioactive plume intercepted rainfall, local deposition of radioactive contamination was higher, even at distances of several hundred kilometres from the plant. This is what distributed the contamination in a surprising pattern of 'leopard spots', which delayed identification of contamination, particularly to the north and east of the Gomel region (Belarus).

A wide-scale detection campaign was implemented to map caesium-137 deposition across the European continent, especially in the most highly contaminated areas, some of which, east of Briansk (Russia), were relatively far away from the emission source (see Figure 34.6). The half-life of caesium-137 is 30.2 years, so it is possible to detect it over the long term, especially since it tends to become fixed in clay; it migrates very slowly unless subject to leaching by heavy rain or flooding. Strontium-90, which is less volatile than caesium, was deposited more rapidly but under the same heterogeneous conditions.

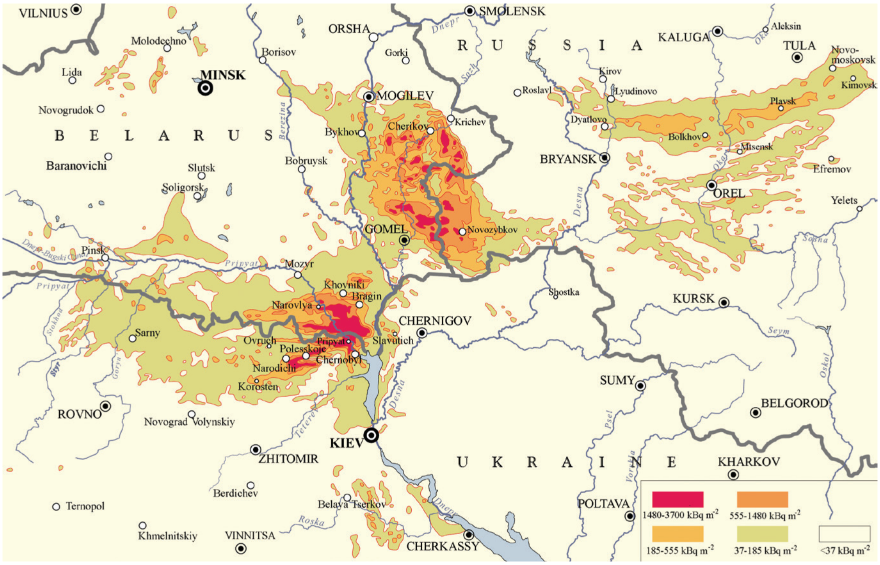


Figure 34.6. Map of soil contamination by caesium-137 in the environment of the Chernobyl nuclear power plant site (from V. A. Borzilov and N. V. Klepikova, Effect of Meteorological Conditions and Release Composition on Radionuclide Deposition After the Chernobyl Accident, in S. E. Merwin and M. I. Balonov (dir.), The Chernobyl Papers. Doses to the Soviet Population and Early Health Effects Studies, Volume I, Washington, Research Enterprises Inc., p. 47-68, 1993).

34.5.2. Protection of the population

There were no inhabitants living within a 3 km radius of the plant. The closest districts of Pripyat, a city with a population of 49,000 inhabitants, were more than 3 km away from the site. The dose rate there began to rise late in the night of 26 to 27 April, reaching 10 mSv/h on 27 April, 24 to 36 h after the accident. Residents were not properly informed until early in the afternoon of 27 April, i.e. about 36 h after the explosions, when stable iodine was distributed and evacuation began. Rumours had been spreading since the night before, but no protective measures had been taken.

Throughout the spring and summer of 1986, approximately 115,000 people who lived within a 30 km radius of the plant, referred to as 'the exclusion zone'[908], were evacuated. Over the next few years, a further 230,000 people were displaced. Comparing the distribution of radioactive release over time, the wind direction map, the map of contamination measured within a 10 to 20 km radius around the site and the location of what became known as the 'Red Forest', a 400-hectare forest of pine trees scorched by extremely high levels of radiation (about 100 Gy), shows that the highest levels of fallout over Pripyat were produced after the population had been evacuated, meaning that they were not among the people the most severely affected.

The authorities and inhabitants of Belarus were not notified immediately and were partially evacuated some time later. The same thing happened in the Bryansk oblast (administrative district) in Russia. People living in these regions did not receive any stable iodine, nor were any restrictions placed on the consumption of food products in the short term. Doses to the thyroid received by these populations were estimated to be ten times higher than doses received by the inhabitants of Pripyat, given that Pripyat had been evacuated.

Regarding the deposition of radioactive contaminants on soil, which contributes to human exposure (not only external, but also internal exposure via the food chain), the contamination maps dating from 1990-1991 show that the Gomel oblast in Belarus was particularly severely affected, especially to the south and northeast. In some places, soil contamination by caesium-137 (see Figure 34.7) was higher than 1.5 MBq/m^2. This was also seen in Russia, in the area surrounding and to the north of Novozybkov. Further still in Russia, the Bryansk, Kaluga, Tula and Orel regions, some 500 km from the site of the accident, were subject to significant caesium contamination (0.2 MBq/m^2).

This distribution of contamination by caesium, which can still be observed given its half-life of 30 years, may not be representative of the distribution of iodine-131 contamination. The release kinetics of these two radionuclides between the time of the explosions and the period during which the graphite burned may have been quite different. In addition, these two radionuclides probably did not behave in the same way in the environment; unlike caesium, iodine may form gaseous species.

Measurements of soil contamination by iodine-129 – which has a long half-life of 15.7 million years – have been taken. Assuming that iodine-129 behaves in exactly the

[908] The official name given to the exclusion zone, which is still in force, is the 'Chernobyl Nuclear Power Plant Zone of Alienation'. It covers an area of 2600 km^2, straddling the border between Ukraine and Belarus. Inhabitants will not be able to return to the area for a very long time. The activity levels of radioactive elements such as caesium-137 and strontium-90 have fallen by only about 50% since 1986. Nonetheless, about a hundred people, or a thousand according to some sources, reside illegally in this zone, which has also been opened up to tourists.

same way as iodine-131, these measurements are needed to establish the most reliable correlations between levels of iodine-131 contamination and thyroid problems, but the maps do not provide a complete picture of the situation.

Available maps also show that within the 30 km exclusion zone surrounding the plant, there was ten times less contamination by strontium-90 (a beta-emitter with low volatility and a half-life of about 29.1 years, which was quickly deposited) than contamination by caesium. Strontium-90 has relatively little effect in terms of external exposure but, if ingested, fixes on bones in the same way as calcium and can cause cancer and changes in the haematopoietic system.

Some plutonium has been detected, with surface activity of a few kBq/m^2 at most, mainly within the exclusion zone.

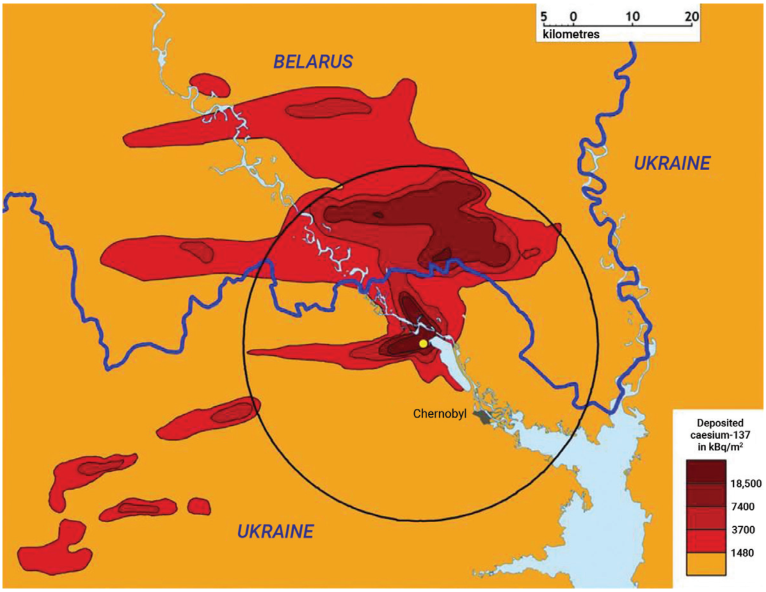


Figure 34.7. Contamination by caesium-137 in the area close to the Chernobyl nuclear power plant. Source EC/IGCE, Roshydromet/Minchernobyl (UA)/Belhydromet, 1998. All rights reserved.

It is interesting to note that while soil contamination levels are often given based on the surface activity of caesium-137 – which has a half-life of 30 years and emits gamma-radiation of 662 keV from its decay product, barium-137m, thereby facilitating detection over the long term – caesium-137 was not the only radionuclide released. It was mixed with iodine isotopes, including iodine-131 (half-life: 8 days), caesium-134 (with a half-life of 2.1 years and showing half the initial surface activity of caesium-137), ruthenium-103 (half-life: 39.3 days) and ruthenium-106 (half-life: 1 year).

Given this combination of radioactive elements and their half-lives, a surface activity of 1000 Bq/m^2 of caesium-137 corresponded to irradiation by external exposure, for a person living continuously in the open air on contaminated land, of 50 μSv in the first year, 30 µSv in the third year, 19 µSv in the tenth year, and 18 µSv in the twentieth year[909].

Outside the exclusion zone, a total of 800,000 people lived in regions where the surface activity of caesium-137 deposition was greater than 0.2 MBq/m^2. Among these people, 33,000 lived in regions where this surface activity was greater than 1.5 MBq/m^2.

Surfaces in urban areas were soon subject to wet deposition due to rainfall, and exposure inside buildings was, at most, 20% of the level outdoors. That made it possible to determine mean exposure for the population groups in question, depending on their lifestyle and living environment. The values applied by the IAEA for the first year were 17 µSv per 1000 Bq/m^2 for Ukraine and 15 µSv per 1000 Bq/m^2 for Russia and Belarus. The value applied for France, which has a smaller farming community and greater urbanization, was 10 µSv/year per 1000 Bq/m^2.

Actual exposure is, of course, directly proportional to actual contamination.

The conclusions of the UNSCEAR 2008 report give the estimated doses for the different population groups as shown in the table below.

Table 34.2. Estimated doses received by populations (UNSCEAR, 2008).

Population group	Population size	Average dose to the thyroid (mGy)	Average effective dose from 1986 to 2005 (mSv)	Collective dose to the thyroid (person × Gy)	Collective effective dose from 1986 to 2005 (person × Sv)
Liquidators	530,000 (*)	Assessment too fragmentary	117	–	61,200
Evacuees	115,000 (**)	490	31	57,000	3600
Inhabitants living in contaminated areas	6,400,000	102	9	650,000	58,900
Other inhabitants of Ukraine, Russia and Belarus	98,000,000	16	1.3	1,600,000	125,000
Other European countries	500,000,000	1.3	0.3	660,000	130,000

(*) This figure includes the 350,000 liquidators in 1986 and 1987, 240,000 of whom were subject to high exposure levels.
(**) The number of people evacuated in 1986.

[909] Calculated using the coefficients given in IRSN’s ECRIN database. ECRIN is a database providing validated and referenced dose coefficients used to calculate doses received by humans. ECRIN covers doses due to external irradiation (exposure to the plume, deposition in soil or immersion in water), and internal contamination by inhalation and ingestion, whether received by workers or members of the public, in different age brackets.

In any event, assessment of the radiological consequences shows that the influence of direct external exposure due to the plume was lower than that of internal exposure due to aerosols and the ingestion of foodstuffs and also lower than external exposure due to deposition (particularly of iodine and caesium isotopes).

34.6. Consequences on human health and the environment

This presentation does not set out to give an account of all the consequences of the Chernobyl accident on people and the environment. While the psychological effects and the impact on the mental health of the population may have been significant, they are not dealt with here. For information on these subjects, readers may refer to the 2006 WHO report mentioned above.

34.6.1. Direct effects of radiation

The Chernobyl accident had the most severe consequences in countries which, at the time, belonged to the former USSR, which was not particularly accustomed to being open about any type of disaster, or even to acknowledging that they might be serious.

Any assessment of the effective consequences of the Chernobyl accident is therefore subject to a lack of accurate and exhaustive data. The information that is most useful is the result of international cooperation which provided, from outside the USSR, the human and financial resources needed to gather data, assisted by medical staff and local authorities. IRSN[910] (initially IPSN) has been deeply involved in these collaborative efforts, for example through the Franco-German Initiative (IFA) for Chernobyl, focused on thyroid cancer in children. This subject will be discussed in Section 34.6.2.

In its 2008 report, UNSCEAR concluded that:

"The observed health effects currently attributable to radiation exposure are as follows:

- 134 plant staff and emergency workers received high doses[911] of radiation that resulted in acute radiation syndrome (ARS), many of whom also incurred skin injuries due to beta irradiation;
- high radiation doses proved fatal for 28 of these people;

[910] In 2007, IRSN published *Les retombées radioactives de l'accident de Tchernobyl sur le territoire français* (Radioactive Fallout in France from the Chernobyl Accident), by Philippe Renaud, Didier Champion and Jean Brenot, Science and Technology Series, published by Lavoisier.

[911] Doses dues to gamma radiation of up to 16 gray to the whole body and 500 gray to skin.

- while 19 ARS survivors died by 2006, their deaths have been explained by various reasons, usually not associated with radiation exposure;
- skin injuries and radiation-induced cataracts are major impacts for the ARS survivors;
- other than this group of emergency workers, several hundred thousand people were involved in recovery operations, but to date, apart from indications of an increase in the incidence of leukaemia and cataracts among those who received higher doses, there is no evidence of health effects that can be attributed to radiation exposure. [...] While there have been indications of an increase in the incidence of cardiovascular and cerebrovascular diseases among the recovery operation workers that correlate with the estimated doses, major concerns over the possible influence of confounding factors [obesity, alcohol consumption and smoking] and potential study biases remain [...];
- the contamination of milk with iodine-131, for which prompt countermeasures were lacking, resulted in large doses to the thyroid in members of the general public; this led to a substantial fraction of the more than 6000 thyroid cancers observed to date among people who were children or adolescents at the time of the accident (by 2005, 15 cases had proved fatal);
- to date, there has been no persuasive evidence of any other health effect in the general population that can be attributed to radiation exposure."

The data presented thus includes the first 28 deaths of the people who received the highest doses, a further 19 deaths which occurred afterwards and are mentioned with reservations as to whether they can be attributed to radiation exposure, and 15 deaths due to thyroid cancer. It should be noted that the first two people who died from multiple trauma (the two operators present on the upper slab of the reactor at the time of the explosion) are not included.

UNSCEAR does not attribute any consequences to the estimated doses received by the general public. Nonetheless, based on a linear non-threshold dose-response model, where the risk of death by cancer is 5×10^{-2} per sievert (a value that remained unchanged between ICRP Publication 60 and ICRP Publication 103 – see Chapter 1) for the three population groups who suffered the highest exposure to radiation, 'projected' figures lead to 3060 cases of cancer in the liquidators, 180 in evacuees and 3945 in people who stayed in the contaminated zones, i.e. a total of about 7000 people. The 1996 report 'predicted' about 8000 cases of radiation-induced cancer for the same population groups; the difference is minimal, keeping in mind uncertainty regarding doses.

The increase in the incidence of non-cancer diseases, such as cataracts or cardiovascular disease, was also reported in certain studies. However, there is no tangible evidence of any increase in these pathologies in the population groups exposed.

To conclude, thirty years after the accident, it is not possible to produce an exhaustive and definitive assessment of the health impact, because the data available are limited due to the quality of the epidemiological studies conducted, the difficulty in precisely identifying who was exposed, and the uncertainty associated with dosimetry estimates. Above all, it was extremely complicated to monitor the public and carry out health checks due to the extent of social and economic upset in the regions in question following the dissolution of the Soviet Union.

34.6.2. Thyroid cancer in children

Spontaneous onset of thyroid cancer is relatively uncommon. The annual incidence rate is approximately 50 cases per million in adults, and two or three cases per million in children. Women are two or three times more likely to develop thyroid cancer than men. Thyroid cancer is fatal in less than 10% of cases.

The increase in the rate of incidence of thyroid cancer following external exposure to radiation had been observed prior to the accident, but there was little information available on the risks associated with internal contamination by iodine-131.

As of 1990, doctors in Belarus began to report a significant increase in the incidence of thyroid cancer in children. Similar data gradually began to emerge in the most heavily affected areas in Russia and in Ukraine, where people had not been promptly evacuated nor been given stable iodine.

At first, this increase – which had not been predicted – met with widespread scepticism among specialists. Now, however, there is no longer any doubt regarding the link between contamination of the thyroid by radioactive iodine and thyroid cancer.

The population group the most severely affected was that of children born before the accident, and especially children aged 10 or under. The annual incidence rate reached 120 per million, i.e. 40 times higher than the annual incidence of spontaneous cancer. Adults were also affected, although the increase in the incidence rate was not as dramatic.

Figure 34.8, based on the IRSN report presenting the conclusions of the IFA for Chernobyl[912] programme, shows the increase in the incidence of thyroid cancer between 1990 and 2000 in children in Belarus, diagnosed in the age range 0-14 years, who were aged 10 or under at the time of the accident. This excess risk disappeared in 2001 since by then, all the children born before April 1986 were no longer in this age range.

Figure 34.8 shows that children exposed to radioactive iodine, who had become young adults, were affected, as were people who were exposed as adults. The excess incidence of thyroid cancer therefore persisted more than 25 years after the accident.

[912] *L'IRSN présente les conclusions de l'Initiative franco-allemande (IFA) pour Tchernobyl* (IRSN Presents the Conclusions of the Franco-German Initiative for Chernobyl), September 2005, available at: https://www.irsn.fr/FR/Actualites_presse/Actualites/Documents/IRSN_conclusions_ifa.pdf.

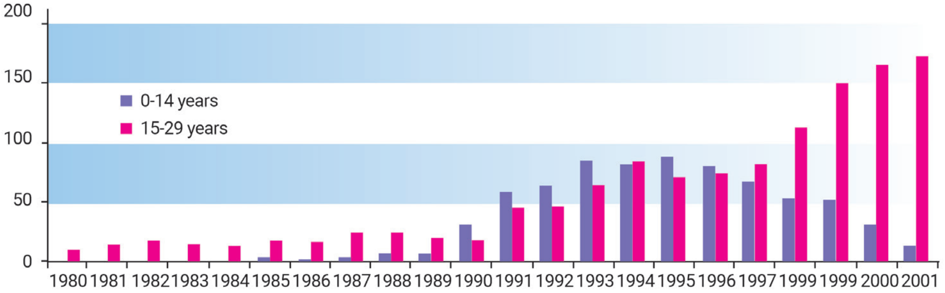


Figure 34.8. Increase in the annual incidence of thyroid cancer in Belarus (for different age ranges at the time of diagnosis) per million people (based on the IFA and the Belarus National Cancer Registry). IRSN.

In the case of people born after 1986, the rate was and remains equivalent to the rate recorded before the accident. So the fact that greater attention was focused on this type of cancer does not explain the results, at least not in Belarus. On the other hand, such attention did lead to earlier detection rates, so the mortality rate decreased.

Similar results were observed in adolescents and young adults in Ukraine and in some highly contaminated oblasts in Russia.

The increase in thyroid cancer in children in Belarus, Ukraine and Russia is shown in Figure 34.9 below, also from the IRSN IFA Report.

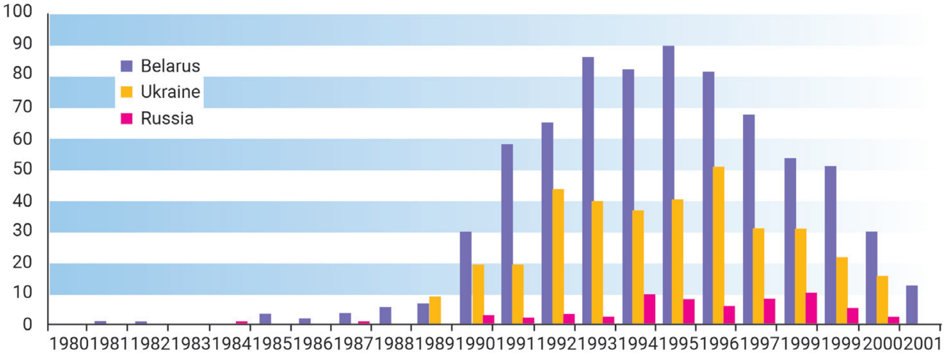


Figure 34.9. Increase in thyroid cancer in children in Belarus, Ukraine and Russia up to 2001 (IFA). IRSN.

As mentioned above, in 2018, UNSCEAR published an updated report on the incidence of thyroid cancer in regions contaminated by the accident at the Chernobyl nuclear power plant (Belarus, Russian Federation and Ukraine) revealing that:

- of a total 19,233 cases of thyroid cancer registered between 1991 and 2015 in people that had been under the age of 18 at the time of the accident, the estimated average number of cases attributable to the accident was about 5000;
- a great deal of uncertainty surrounds this estimated average, as the number of cases attributable is between 700 and 10,000 cases.

34.6.3. Long-term contamination in the Dnieper Basin

Tonnes of material were propelled out of the reactor core by the explosions. This was either bulldozed over during clean-up of land at the base of the damaged reactor or buried in about 800 storage trenches around the site. This debris was not protected from washout by rainwater running down through the soil nor from rising groundwater. Contamination could therefore migrate through the soil by dissolution, and then be transported by groundwater to waterways and surface water bodies. These phenomena occur slowly, but surely.

A plan was developed to slow radionuclide migration by constructing a geotechnical barrier in the ground, encircling the most highly contaminated zone containing the four reactor units. Work began on this barrier in 1986 downstream of groundwater flow. It was stopped when it was found to cause a significant rise in the groundwater level, since rainwater and water from major leaks in the service water systems used to cool the condensers had no other outlet. The rise in groundwater level that would have resulted from sealing off the most severely contaminated area would have flooded the plant unit basements, which would obviously have made it impossible to continue operating. Construction work on this barrier was therefore stopped.

In 2006, the IAEA published a report on radiological conditions in the Dnieper Basin[913] and their evolution.

One kilometre from the plant, a large cooling pond (150,000 m^3) had been built for use as a heat sink for the different reactor units at the plant. It was supplied by pumping water from the Pripyat River and was separated from it by a dam, downstream of the pond.

This cooling pond became severely contaminated, particularly by the 5000 m^3 of water discharged into it from the basement beneath the damaged reactor. It contains over 200 TBq of radionuclides, most of which are concentrated in the sediment in the river basin. They are migrating by several centimetres a year toward the Pripyat River which then runs into the Dnieper River Basin. If the flow control gates downstream into the Pripyat River are not managed correctly, or in the event of failure of the downstream dam, radionuclide transfer could suddenly increase at a much faster rate.

[913] Radiological Conditions in the Dnieper River Basin, Radiological Assessment Reports Series, IAEA, 2006.

Of all the watercourses in the Dnieper Basin, it is obviously the Pripyat River – whose catchment drains the most severely contaminated areas in Belarus and Ukraine – that shows the highest levels of contamination.

A significant portion of the 30 km exclusion zone surrounding the site is a floodplain, which floods several times a year, especially due to snowmelt. Surface deposition, mainly of caesium and strontium, since iodine is no longer significant due to radioactive decay, is regularly washed out by flooding. This has reduced local concentrations, but increased concentrations in the lakes and ponds in the zone, and dispersed the contamination downstream. Fish in the lakes and ponds are highly contaminated.

Monitoring concentrations of caesium-137 and strontium-90 in Dnieper River water reveals the effects of rises in river level and flooding, as well as how caesium becomes fixed in sediment.

Since the late 1990s, concentrations of these two radionuclides in the water of the catchment basin supplying Kiev have been low enough to classify this water as potable (see Figure 34.10).

Approximately 90 TBq of strontium-90, i.e. 1% of the amount released, were transported as far as the Black Sea; in the year 2000, concentrations could still be measured in the water at the mouth of the Dnieper.

For caesium-137, about 4 TBq, or 5 × 10^{-5} of radioactive release inventory, has been transported to the Black Sea. Since the mid-1990s, concentrations of caesium-137 have not been high enough to distinguish them from background radiation.

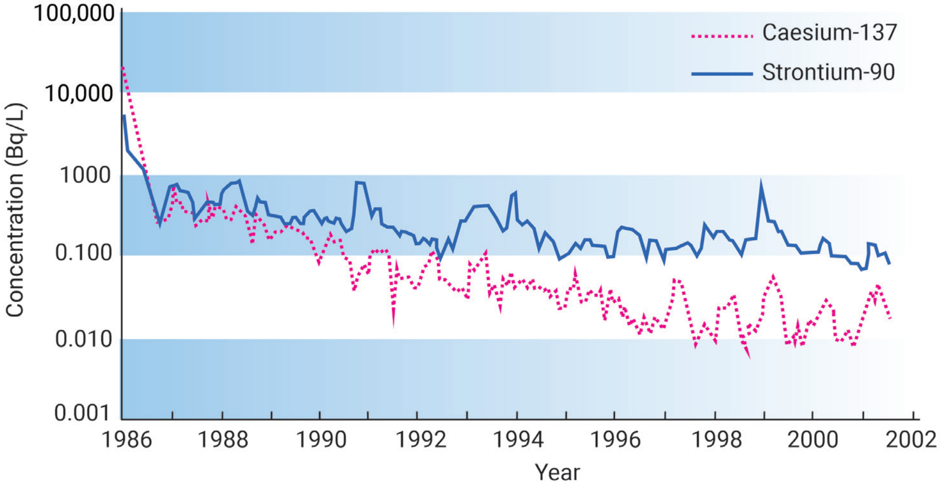


Figure 34.10. Concentrations of caesium-137 and strontium-90 at the Kiev dam (1986-2001). IRSN (source IAEA, 2006 [see Footnote 913]).

34.7. Radioactive fallout in France and its consequences

In 2007, IRSN published research[914] updating knowledge on radioactive fallout in France from the Chernobyl accident and its consequences; this research was again updated in 2016[915]. This subject is discussed briefly below, but readers may refer to these works for more precise information.

34.7.1. Doses attributable to the plume

France was most severely affected by radioactive release on 27 April 1986, borne on easterly and then south-easterly winds. Activity levels in the air rose suddenly from 30 April to 1 May, especially in north-eastern France. The mean activity concentration of caesium-137 in the air from 1 to 5 May 1986 ranged between a few Bq/m^3 to less than 0.15 Bq/m^3 from east to west.

Extensive measurements of plume content by IPSN at its atmospheric aerosol sampling station in Verdun, where the highest mean concentrations were observed (5.5 Bq/m^3 of caesium-137 on 1 May), were used to measure doses by inhalation and by external exposure due to the plume. For Verdun, the effective dose via inhalation was an estimated 46 µSv in adults; the equivalent dose to the thyroid in infants aged 1, the most sensitive age, was an estimated 470 µSv. At the same site, doses by external exposure attributable to the plume were much lower than the values above.

Further to the west and to the south, doses were lower: ten times lower in the Cotentin region, for example.

34.7.2. External doses due to soil deposition

Radionuclide deposition is highest when it rains. Based on measurements of residual radioactive deposition conducted across the entire eastern side of the country, and linking deposition activity levels with rainfall between 1 and 5 May 1986, IRSN mapped deposition throughout France (see Figure 34.11). The resulting maps show extremely contrasting values in different regions of France, with much higher and very heterogeneous levels of caesium-137 deposition in the eastern third of the country, peaking in places at 20,000, and even 40,000 Bq/m^2 as a result of precipitation, which was also very heterogeneous across this area, and lower and more uniform deposition (less than 5000 Bq/m^2) across the rest of the country.

[914] Philippe Renaud, Didier Champion, Jean Brenot: *Les retombées radioactives de l'accident de Tchernobyl sur le territoire français* (Radioactive Fallout in France from the Chernobyl Accident), Science and Technology Series, published by Lavoisier, 2007.

[915] *1986-2016:Tchernobyl, 30 ans après/Impacts de l'accident de Tchernobyl en France et en Europe* (Chernobyl 30 Years Later/Impact of the Chernobyl Accident in France and Europe), IRSN website, 2016.

In 2002, the CRIIRAD[916] published an atlas of contamination in France based on in situ measurements taken in 1999 and 2000, thus supplementing earlier measurements. Similar results were produced using both these approaches.

It was mentioned above that a caesium-137 surface activity of 1000 Bq/m^2 corresponds to a mean external exposure of 10 μSv in the first-year. Therefore, for a person residing in one of the places affected by the highest levels in France (40,000 Bq/m^2 of caesium-137), the external dose attributable to radioactive deposition reached 400 μSv for the year 1986 – i.e. 25 times lower than the doses observed in people who were not displaced from areas close to Chernobyl.

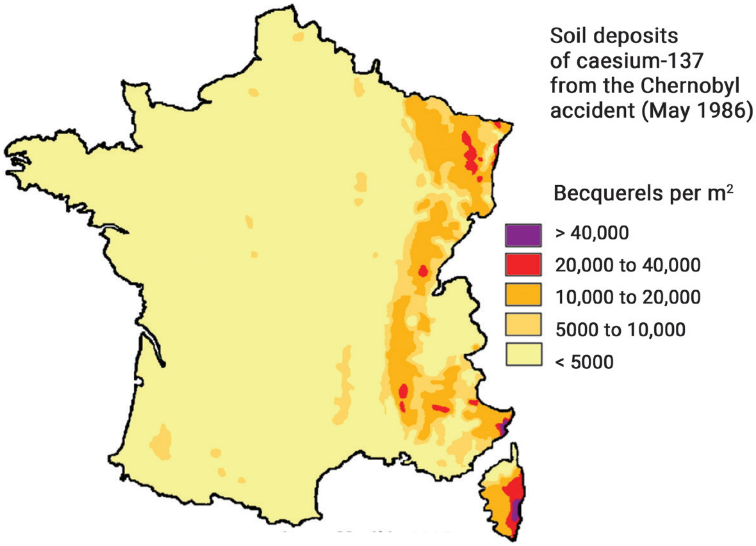


Figure 34.11. Caesium-137 deposition in France reconstituted by IRSN (updated, 2005 model). IRSN.

34.7.3. Doses due to ingestion of contaminated foodstuffs

The document published by IRSN in 2007, mentioned above, describes the various mechanisms that needed to be considered in order to assess doses due to the ingestion of contaminated foodstuffs.

The highest levels of contamination observed in foodstuffs were observed immediately after deposition, especially in leaf vegetables (lettuce, spinach, cabbage, etc.) and milk (see Figure 34.12), followed by beef. These vegetables and pasture grass received radioactive deposition directly on the leaf surface. Activity levels then dropped rapidly (due to radioactive decay in the case of iodine and to plant growth in the case of

[916] *Commission de recherche et d'information indépendantes sur la radioactivité* (Commission for Independent Research and Information on Radioactivity).

caesium). Mean effective doses received in 1986 in adults ranged from about 300 µSv in eastern France to less than 50 µSv in the west.

Annual effective doses subsequently fell. As of 1987, crop and animal farmland was primarily contaminated via the soil; this long-term contamination is much lower than contamination via deposition on leaf surfaces in May 1986.

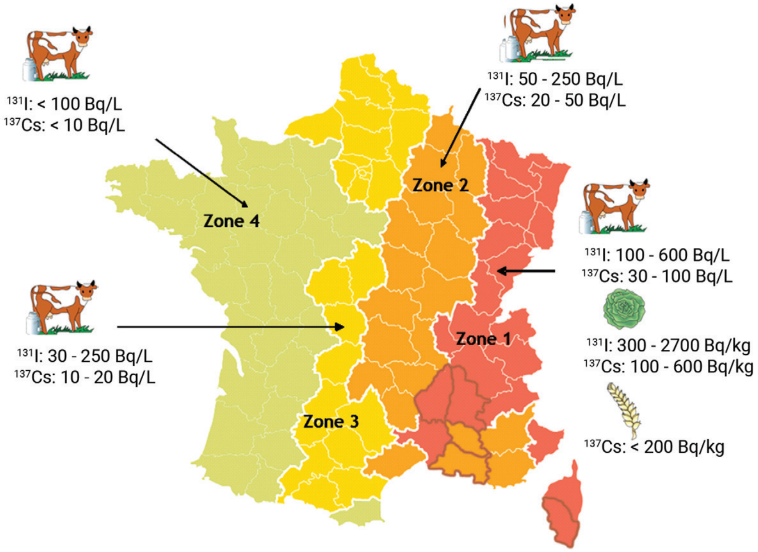


Figure 34.12. Ranges of caesium-137 and iodine-131 contamination levels in the first two weeks of May 1986, in leaf vegetables, milk and cereals. IRSN.

34.7.4. Overall levels

In the mid-2010s, there were still some areas of France where radiation levels were higher or even much higher than those observed in the rest of the country. Referred to as ‘residual artificial radioactivity zones’, these areas can be identified because of the caesium still present in contaminated soil. Surface activity exceeded 10,000 Bq/m^3 in areas affected by the Chernobyl accident (areas that had seen the heaviest rainfall in the days following the accident)[917] and 3000 Bq/m^3 in areas affected by fallout from atmospheric nuclear weapons testing in the past.

In foodstuffs, caesium-137 levels in milk sampled from residual activity zones (average 0.32 Bq/L) were higher than levels in milk sampled in other areas (maximum 0.03 Bq/L).

[917] In grasslands in the southern Alps, a number of hot spots were identified covering very small areas but with activity greater than 100,000 Bq/m^3.

The cumulative effective dose for the period 1986 to 2006 due to fallout from the Chernobyl accident was an estimated 4.5 mSv in adults[918] living in the most highly contaminated areas in France. That was less than a tenth of the average dose due to background radiation over a period of 20 years. Of this cumulative dose, 30% was received in 1986 and 1987. The fraction received in 2006 was just 1%. For western France, the values were ten times lower.

Figure 34.13 below shows consistent decreases in estimated annual doses in France (in mSv/year) from 1986 to the mid-2010s.

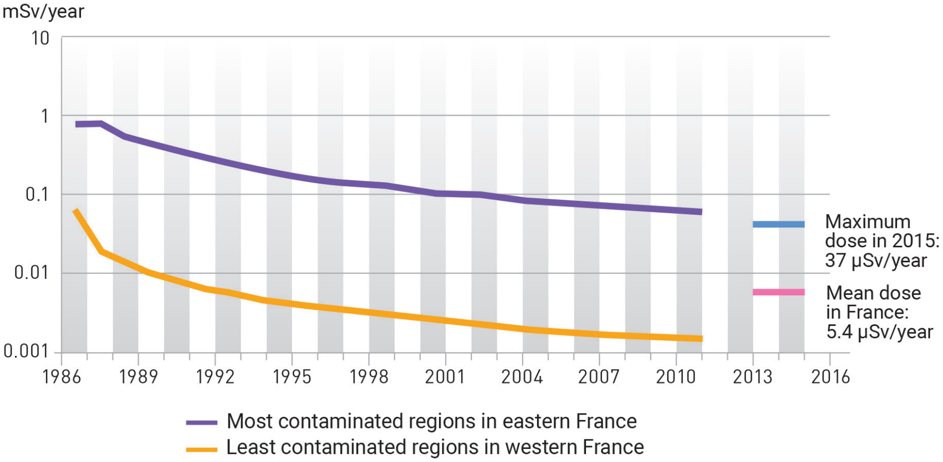


Figure 34.13. Assessment of mean effective doses attributable to fallout from the Chernobyl accident in France up to the mid-2010s (external exposure and exposure by ingestion). Kazoar Agency/IRSN.

34.7.5. Thyroid cancer

The French Institute for Public Health Surveillance (*Institut national de veille sanitaire*, InVS[919]) conducted epidemiological studies to assess the incidence of thyroid cancer in France and trends in French *départements* which keep relevant registers, and also in Corsica. These studies were presented in reports published in 2011[920] and 2012[921], respectively.

[918] The effective doses received by adults are always higher than those received by children because they eat larger quantities of food and spend more time outdoors.

[919] Now part of the French national public health agency, *Santé publique France* (Public Health France) (since 2016).

[920] A. Rogel et al.: *Évolution de l'incidence du cancer de la thyroïde en France métropolitaine – Bilan sur 25 ans* (Changes in the Incidence of Thyroid Cancer in Mainland France — Analysis over a Period of 25 Years), InVS, 2011.

[921] L. Pascal, J. L. Lasalle: *Estimation de l'incidence du cancer de la thyroïde en Corse*, 1998-2006 (Estimation of the Incidence of Thyroid Cancer in Corsica from 1998 to 2006), InVs, 2012.

34.7.5.1. Monitoring thyroid cancer in France

The system organized to monitor thyroid cancer is primarily based on cancer registers: 15 French *départements* are covered by general registers. Since 1975 a special register has kept records of thyroid cancer cases in the Marne and Ardennes *départements*. These registers covered about 20% of the population of France for the period 1982-2006. In addition to this system, monitoring is based on healthcare administration databases (health insurance databases and hospital databases), which are readily accessible.

The results were presented in the study by A. Rogel (InVS) published in 2011 (see Footnote 920). For the purposes of this study, the decision was made to monitor changes in papillary carcinoma, the most common form of thyroid cancer, which saw the most rapid increase and was the most likely form to be diagnosed following exposure to iodine-131. Results for the period from 1982 to 2006 were available for nine *départements*.

Between 1982 and 2006, the increase in the incidence of thyroid cancer was significant for both genders, with a mean average annual increase of 6%. There was an even greater increase in cases of papillary thyroid carcinoma, which increased at an average annual rate of more than 8% per year for both genders.

The increase in the incidence of thyroid cancer slowed over the period 2002-2006 compared to the period 1982-2002, increasing at a slower rate and with no difference between men and women. This trend was largely related to the fact that the rate of increase in the incidence of papillary thyroid carcinoma began to fall as of 2001.

Results were presented in the study by L. Pascal (InVS) in 2012 (see Footnote 921), covering two shorter periods, 1998-2002 and 2003-2006, for a larger number of *départements*. The Bas-Rhin, Haut-Rhin, Isère and the Doubs in eastern France are included in Zone 1, the Ardennes, Marne and Hérault are in Zone 2, Somme and Tarn are in Zone 3, Calvados, Manche, Loire Atlantique and Vendée, all of which are further west, are in Zone 4. This study shows that the two *départements* in Alsace have the lowest incidence, while the Vendée is one of the *départements* with the highest incidence (up to 6 per 100,000 with a 95% confidence interval for men and 20 per 100,000 for women). While the incidence in Isère was significant during the second period for both men and women, it was much lower during the first period.

This implies that there was no correlation between these results and iodine-131 ingestion through food in 1986, since radioactive fallout over the Vendée region was significantly lower than it was over Alsace.

In the case of Corsica, L. Pascal's study shows a higher incidence of thyroid cancer than in mainland France only during the period 1998-2002 and for men (incidence up to 10 per 100,000 with 95% confidence interval). The incidence of cancer in Corsica subsequently fell to the same level as in Isère and Vendée.

34.7.5.2. Assessment of the number of cancer cases induced in France by the Chernobyl accident

The highest probability of developing thyroid cancer was found in children born in the 15 years before May 1986 and who lived in 25 *départements* in eastern France (Zone 1 in red on the map in Figure 34.12). Records show that there have been 2.27 million such cases.

Equivalent doses to the thyroid in children who lived in Zone 1 in Figure 34.12 are given in Table 34.3. These doses were caused by iodine-131 (in over 90% of cases) and by iodine-132 (from tellurium-132) and were received in the three months immediately following the deposition of radioactive substances. Behind these average figures, found for standard eating habits and practices, there lies a significant amount of variability, mainly relating to how fresh the produce consumed was. For instance, a person who only eats processed foodstuffs (long-life milk, canned and frozen food) will have received a much lower dose, regardless of where they live.

Table 34.3. Equivalent dose to the thyroid according to age in 1986.

Children age groups	3 months	1 year	Age 5 to 9	Age 10 to 14
Equivalent dose to the thyroid (mGy)	1.9 ± 0.6	9.8 ± 3.2	6.0 ± 1.9	2.9 ± 0.9

Based on these dose estimates, IRSN conducted a quantitative evaluation of thyroid cancer risk. This evaluation used non-threshold dose-response relationships drawn from the scientific literature to estimate, by calculation, the number of cases attributable to a given exposure value.

Given that there is a latency period between exposure of the thyroid to ionizing radiation and the development of thyroid cancer, evaluations of the number of cases of spontaneous cancer (due to other causes) and the ‘expected’ numbers of excess cases resulting from the Chernobyl accident cover the periods 1991-2000 and 1991-2015.

Table 34.4. Estimated number of cases of ‘spontaneous’ thyroid cancer and confidence intervals for the number of excess cases of cancer in people aged 15 and under in 1986 living in Zone 1.

Period	Number of spontaneous cancers	Number of excess cancers	Percentage of cases ‘in excess’ in relation to the number of spontaneous cancers
1991-2000	97 ± 20	between 0.5 and 22	0.5 to 23 %
1991-2015	899 ± 60	between 6.8 and 55	0.8 to 6 %

These results show that the estimated number of excess cases is lower than or comparable to the estimated number of cases of spontaneous cancer, implying that excess cases are not easily detected by means of epidemiological studies.

34.8. Lessons learned by the international community from a general viewpoint and with regard to RBMK reactors

First, in discussions held after the Chernobyl accident, it was generally agreed that a more international vision of nuclear safety was necessary, reflected particularly in the various reports published by INSAG, the international group of experts in nuclear safety, at the time recently created within the IAEA[922]. These included the INSAG 1986 report entitled, Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident (Safety Series No. 75-INSAG-1), in which the concept of **safety culture** was first developed, before being developed in greater depth in 1991 in the INSAG report on Safety Culture (Safety Series No. 75-INSAG-4). In 1992, the INSAG-1 report was revised, leading to the INSAG-7 report.

Regarding the RBMK reactor series in particular, in addition to the modifications mentioned in Section 34.3, some more general lessons were also learned, including the following:

– operating experience feedback was not being adequately shared between operators and designers; apart from the incident at the Ignalina plant in 1983 mentioned above, which had not resulted in any changes or restrictions placed on RBMK operating procedures, another incident had occurred in 1975 at Unit 1 of the Leningrad nuclear power plant, which can be thought of as a precursor to the Chernobyl accident. This incident ended in a pressure tube failure resulting from a sequence of events that was not unlike the one leading up to the Chernobyl accident, namely prolonged operation at half-power, followed by complete shutdown, just prior to the reactor being reconnected to the grid. The incident included xenon poisoning in the core, major disruption in neutron flux distribution, operators who obstinately proceeded with power build-up, an inadequate operating reactivity margin (equivalent to less than 15 control rods inserted in the core), all of which probably resulted in a nuclear power excursion limited to a specific part of the reactor. The operators at the Chernobyl nuclear power plant had never heard anything about the nature or the causes of this incident;

– the inspection and authorization system in the former Soviet Union was inadequate. The Soviet investigation commission itself found that the Chernobyl plant failed to comply with the Soviet safety regulations and standards in force even at the time of its construction, in the mid-1970s;

– operating personnel needed documentation clearly describing procedures that did not contradict each other. They also needed to comply with operating rules (including rules regarding disabling of the safety systems) and test procedures, or, at least not deviate from the rules and procedures without first conducting a safety assessment in cooperation with competent staff.

[922] See Chapter 3.

Changes were subsequently made to safety organization and to authorization and inspection methods and procedures in Soviet Union countries.

More specifically, with regard to training for operating crews, simulator-based training was introduced, covering all situations, including severe failure conditions.

Training for operating crews was gradually improved to the level that seems to have been lacking at the time when they disconnected the safety systems and pursued operation outside the permissible operating domain.

34.9. Lessons learned in France

With regard to any technical design improvements that could be made, RBMK reactors were too unlike the type of reactor used in France for these to be directly relevant. Nonetheless, the information obtained in the months following the Chernobyl accident led to various questions being raised and initiatives launched with regard to the reactors in service in France, which it is useful to recall here.

Power reactors operating in France have fast-acting automated reactor shutdown systems and include the option of performing a manually-operated trip.

Fast-neutron reactors, which have all been taken out of service in France since 2009, do not come within the scope of this work. It is nonetheless interesting to mention a few points where certain similarities with RBMK reactors were investigated in light of the Chernobyl accident, during which, as pointed out previously, the positive void coefficient of the coolant was a determining factor. Although an insertion of reactivity could indeed have occurred in fast-neutron reactors in the event of the (liquid sodium) coolant boiling or draining, a major difference between fast-neutron reactors and RBMKs is the fact that the sodium was not pressurized in the former and that, under normal and incident conditions, it remained at a temperature approximately 300°C less than its boiling temperature. Under certain accident conditions, there was a risk of reaching local boiling, but the reactor would be tripped by the safety system before it could reach generalized boiling. Fast-neutron reactors were equipped with individual thermal monitoring sensors on each fuel assembly and with multiple reactor shutdown systems. Furthermore, the decree authorizing the construction of France's PHENIX and SUPERPHENIX reactors included the requirement that a core-melt accident involving a release of energy must be taken into account in their containment design.

Water-cooled reactors are not subject to a power rise if the coolant reaches the boiling point or if a loss of coolant occurs. However, a further study programme to investigate possible reactivity accidents that had not been considered at the design stage was conducted in a collaborative effort involving Électricité de France (EDF), Framatome and IPSN. This programme identified a first accident sequence of concern, presented in the next chapter. The study programme was extended to review all earlier studies on reactivity accidents in order to check whether they were consistent and exhaustive, seeking any available margins (such as studying the rapid withdrawal of two or three control rods rather than just one), as well as seeking any possible new sequences under different operating states and under accident conditions.

Other subjects were also studied specifically in light of feedback regarding the Chernobyl accident, including:

- safety culture,
- the possibility of disabling safety functions and engineered safety systems,
- the possibility of providing on-site emergency response in the event of a severe accident.

These subjects were also examined for facilities other than nuclear power reactors.

In France, operator training, the composition of operating crews when specific tests are carried out, and procedures for assessing and authorizing such tests have all been recognized as factors that can contribute to preventing a sequence of events such as the one that led to the Chernobyl accident.

It was observed that postponing the test programme[923] affected some of the conditions in which the test was to be conducted at Unit 4 of the Chernobyl nuclear power plant, altering the level of xenon poisoning in the core and, in turn, the operating reactivity margin. The impact of any changes in the timing of activities can vary greatly. Two activities that are incompatible, at least as regards the operational limits and conditions, may end up being carried out at the same time. This is an important lesson for everyone, especially in managing reactor shutdown situations.

Regarding the possibility of disabling safety systems, IPSN, in cooperation with EDF, carried out an in-depth assessment of the ability of systems and humans to respond to an operating situation where safety systems have been disabled, and other cases where operational limits and conditions have not been applied, in order to identify the causes of these situations and define appropriate corrective measures. Assessment of the possibility of disabling systems placed focus on automatic protection functions and engineered safety features (emergency shutdown system, safety injection system, containment spray system), describing:

- intentional inhibition of a system, decided by the operator (for example, for test or maintenance purposes) and indication of system inhibition,
- the means required to alert operators if a system is unintentionally inhibited.

The assessment provided the opportunity to identify or confirm practical aspects including:

- how information regarding the disabling of equipment is reported to the control room;
- preventing system line-up errors (valve position errors, etc.) and measures designed to detect them, an issue that had been dealt with previously following the accident at Three Mile Island, and had led to improvements including the

[923] The request coming from services outside the facility to increase the power supply to the grid came just after the test had begun, interrupting the programme for nine hours.

installation of limit-switch sensors to report valve position information to the control room;

- the operating rules applicable under cold shutdown conditions, which allow certain parts of protection functions and engineered safety features to be disabled, for example, for preventive maintenance purposes. Already in 1983, a review had demonstrated that for a given time period, the number of significant incidents that occurred during cold shutdowns was disproportionately higher than at power, explained by the significant amount of maintenance operations undertaken during cold shutdowns. Stricter cold shutdown operating rules were implemented in the summer of 1986;
- whether or not equipment lockout was adequately checked, given that there are over a thousand equipment lockouts on a reactor every year. The Chernobyl accident also led to a review of the risks of forgetting to restore all equipment items to an operational state after a lockout.

The most important lessons learned from the accident at the Chernobyl nuclear power plant, however, are related to broader issues. Safety culture, for one, as mentioned above, and the practical aspects of managing a site with several reactor units when one of them is in an accident situation. From a broader viewpoint, there is also the question of post-accident management. The scale of the resources required to manage the aftermath of such an accident is impressive: measuring radioactivity levels in facilities, at the site and in the environment, providing the ability for responders to take action on site and at the damaged reactor, controlling fires under highly-radioactive ambient conditions, evacuating large numbers of people, treating those who have been seriously exposed to radiation, protecting populations from the spread of radioactive contamination, clean-up of vast areas that have been contaminated, monitoring food chains and monitoring the health of affected populations. The accident at the Fukushima Daiichi nuclear power plant in March 2011 was a stark reminder of the importance of these concerns (see Chapter 36).

After the Chernobyl accident, in 1988, French nuclear operators all joined forces to form an economic interest group, the *Groupe d'intervention robotique sur accident* (INTRA[924], providing post-accident robotic response solutions), to develop, operate and maintain remote-controlled robotic equipment capable of being deployed 24 h a day, 7 days a week in the event of a large-scale nuclear accident at facilities belonging to the three member organizations. It is based at the Chinon nuclear power plant site.

In 2005, under the provisions of an interministerial directive, the *Direction générale de la sûreté nucléaire et de la radioprotection* (French Directorate-General for Nuclear Safety and Radiation Protection), which has since become the *Autorité de sureté nucléaire*, or ASN (the French Nuclear Safety Authority), was tasked with defining the framework and identifying, planning and implementing measures required to respond to post-accident situations following a nuclear accident. This led to the creation of the *Comité directeur*

[924] Consult the website at https://www.groupe-intra.com/eng. This group was founded by EDF, CEA and Orano.

pour la gestion de la phase post-accidentelle d'un accident nucléaire (CODIRPA) (Steering Committee for Managing the Post-Accident Phase of a Nuclear Accident or Radiological Emergency). CODIRPA brings together national and local stakeholders, including public authorities, plant operators, associations (such as ANCCLI, the French National Association of Local Information Commissions and Committees, etc.), and assessment bodies including *Santé publique France*, IRSN, etc. Within this committee, various working groups are tasked with developing policy on subjects such as taking emergency measures to protect the public, reducing contamination in a built environment, living conditions in contaminated rural areas, issues relating to water (impact of the accident, managing water resources), waste management, public health monitoring, and assessing radiological and dosimetric consequences. CODIRPA published its first policy document[925] in 2012.

A large number of research programmes have also been conducted to improve models of radionuclide dispersion and deposition resulting from airborne release. This chapter has provided several examples where these models have been used.

Last, another key area, although far removed from the more purely technical aspects, is communication and keeping the public informed, where the difficulties encountered have led to reflection on the need for greater transparency in the area of nuclear safety and radiological protection.

34.10. Keeping the public informed

In the days immediately following the Chernobyl accident, and even more so in the months that followed, it was seen just how difficult it was for the general public and those in charge of informing the public to form an accurate picture of the relative severity of any reported incident, accident or even a simple anomaly at a nuclear power plant.

The selection criteria used to identify safety-related events and significant incidents (or events) (see Chapter 21) are mainly focused on the potential consequences of events and whether or not they may be precursor events leading to severe situations affecting the reactor. They cannot be used directly to describe events to a non-specialized audience.

In 1987, the French authority responsible for nuclear safety and information, the CCSIN (*Conseil supérieur de la sûreté et de l'information nucléaires*) proposed establishing an event scale that could be easily understood, rating incidents on the basis of factual criteria.

A working group consisting of journalists and representatives from EDF and safety organizations was set up for this purpose. In 1988, inspired by the scales used to describe earthquake magnitude, they proposed a scale for rating the severity of incidents and accidents at nuclear power plants. From the beginning, it was made clear that this scale was not intended to be used in safety analyses, but should be seen as

[925] *Éléments de doctrine pour la gestion post-accidentelle d'un accident nucléaire* (Policy Elements for Post-Accident Management in the Event of a Nuclear Accident), ASN, October 2012 (http://www.asn.fr).

a separate additional tool for facilitating communications outside highly-specialized communities, by focusing on the relative significance of different types of event. The levels ranged from 1 (minor incident) to 6 (major accident), depending on criteria such as the consequences both inside and outside the nuclear facility site or any weakening of defence in depth.

This scale preceded the INES scale, which was the outcome of discussions at international level. These discussions and the initial conclusions drawn were subsequently taken up by the OECD and the IAEA to define the International Nuclear Event Scale – INES. The first version, focused on nuclear power plants, was used starting in the early 1990s.

In comparison to the scale proposed in France, the INES scale includes Level 0 for events that have no impact on safety and Level 6 for events in between accidents such as Three Mile Island (Level 5) and Chernobyl; the Chernobyl accident was reclassified as a Level 7 event (the Fukushima Daiichi nuclear power plant accident was also rated a Level 7 event).

The INES scale was subsequently extended to cover every type of facility within the civil nuclear industry. Since the 2000s, it has continued to be adapted in response to the growing need for communication regarding the significance of events relating to the transportation, storage and use of radioactive materials and radiation sources. Figure 34.14 gives a very simplified representation of the INES scale. A manual published by the IAEA (The International Nuclear and Radiological Event Scale – User's Manual, 2008 Edition) sets out how the scale should be applied – specifying certain radiological dose rate limits for classifying events involving people exposed to radiation.

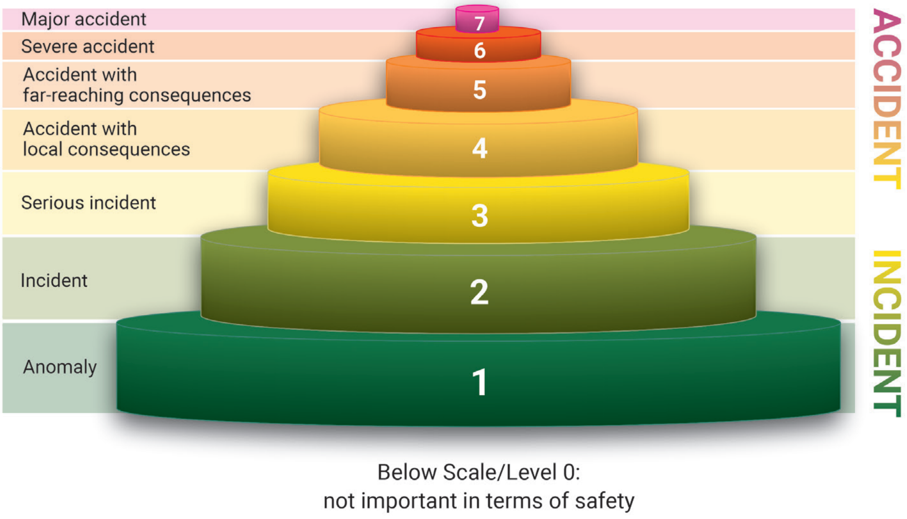

Major accident
7
Severe accident
6
Accident with far-reaching consequences
5
Accident with local consequences
4
Serious incident
3
Incident
2
Anomaly
1
ACCIDENT
INCIDENT
Below Scale/Level 0:
not important in terms of safety

Figure 34.14. Keeping the public informed on events occurring at nuclear facilities: the INES scale. Georges Goué, IRSN.

Again, it is important to emphasize that this scale is intended to be an easy-to-use tool for providing information to the general public. It should not be used as an indicator of safety conditions at various facilities or in different countries, which would seriously defeat the purpose of calmly and clearly reporting on events and classifying their impact.

Regardless of the circumstances, INES should be used with caution to avoid any possible misleading comparisons. In France, operators must report all events (nuclear incidents and accidents) to ASN, the French Nuclear Safety Authority, within 48 working hours and include a proposed INES rating. The proposed rating is examined by ASN (usually in cooperation with IRSN), which makes the final decision on the rating given. ASN uses this scale to select, out of all the events that occur, those that are significant enough to require communication on its part:

– ASN only issues an incident report on an event rated INES Level 0 if there is a specific reason for doing so;

– ASN systematically publishes an incident report on events rated INES Level 1 on the ASN website;

– ASN issues a press release on any event rated INES Level 2 or above and also notifies the IAEA.

34.11. After the Chernobyl accident

To conclude, the accident at the Chernobyl nuclear power plant did not fundamentally call into question the safety principles applied in the design of nuclear power reactors in the West.

However, where the Three Mile Island accident led to shifting the prospect of a core-melt accident from a mere outcome predicted by simulation code to an actual possibility, the Chernobyl accident transformed all the theoretical equations on the release of fission products and models of atmospheric dispersal into a tragic long-term reality impacting people's lives, with confrontations between experts and continent-wide political wavering.

It also revealed a clear need to improve safety at all nuclear facilities worldwide and led to studies and research that have resulted in new knowledge in such complex subjects as:

– reactivity accidents in water-cooled reactors,

– severe accidents,

– the transfer of radioactive substances to the air, soil and foodstuffs,

– the impact of ionizing radiation on human health and the environment.

The Chernobyl accident also revealed the complexity of questions raised by long-term contamination of land in the event of a severe accident in a nuclear reactor and led to a number of initiatives on the subject – such as founding of CODIRPA in France, as mentioned above.

Videos available for viewing

The Chernobyl Plume, subtitled in English

Modelled Displacement of the Chernobyl Plume

Contaminated Land Around Chernobyl (in French)

The Chernobyl Sarcophagus (in French)

Chapter 35

Options and Control of Reactivity Insertion in Pressurized Water Reactors

As indicated in Chapter 5, reactivity in a nuclear reactor must be controlled at all times. This fundamental safety function has nonetheless been jeopardized on several occasions, notably in 1986 during the accident at Unit 4 of the Chernobyl nuclear power plant, described in the previous chapter.

This chapter presents the measures taken to prevent the risk of uncontrolled reactivity insertion[926] in a pressurized water reactor. This kind of reactivity insertion in an operating reactor is called a reactivity incident or accident. If it occurs when the nuclear chain reaction is not desired (in a fuel storage area or in a reactor core in a state of extended outage, particularly if the reactor coolant system is open), it is considered a criticality accident.

In the days following the Chernobyl accident, IPSN organized a team whose task was to understand the causes of the accident and determine the lessons to be learned. By early July 1986, it had found various aspects that required study. However, the causes of the accident were not fully identified until several months later, when Russian scientific experts published their findings. The main finding was that the accident was made possible by a series of safety rule violations and the inhibition of certain protection functions. Some intrinsically unfavourable characteristics of RBMK

[926] The terms ‘insertion’, ‘injection’, and ‘introduction’ all mean the same thing when referring to adding reactivity in the core, which increases the number of fissions and thereby, nuclear power.

reactor cores also played a role. Together, these causes led to a reactivity accident (see previous chapter).

In France and internationally, stakeholders expressed their intention to ascertain all the lessons that could be learned from this accident, particularly in terms of emergency response. However, given the differences in design and operation, it did not seem that the fundamental safety principles of Western power reactors would be called into question. In particular:

– in normal operating conditions of a pressurized water reactor, an increase in power or temperature leads to a decrease in reactivity which tends to curb the increase in power;

– the insertion of control and shutdown rod cluster control assemblies (RCCAs) always reduces core reactivity; their drop time is much shorter than for an RBMK reactor (2 s compared to 20 s when the accident occurred);

– it is not common practice to inhibit safety systems for electricity generation reasons or to successfully perform a test.

However, after such a significant accident, it seemed necessary to re-examine all studies supporting the safety analysis reports for French reactors, focusing in particular on the potential consequences of non-compliance with operating rules. A group of experts from Framatome, Électricité de France (EDF), and IPSN thus began to consider the possibilities of accidents like the Chernobyl accident occurring in a pressurized water reactor, even though the consequences could not be as significant, in theory, given the design differences.

The objective was to determine the conditions in which situations of this type could occur, independently of whether or not the scenario was plausible. The main concern was therefore to identify risk situations in order to understand the physical phenomena that could mitigate the ensuing consequences. Whether these situations should be taken into account could then be discussed in a second phase. To gain new insight, the first step was to 'return to physical phenomena' by considering those phenomena that could introduce reactivity in the pressurized water reactor core, without referring to identified scenarios or earlier studies, and even less to probabilities. Certain postulated scenarios had a probability significantly below 10^{-7} per reactor and per year, the limit generally adopted at that time (per event family) for considering a scenario in the design phase.

As part of this analysis, the possible variations of each reactor parameter and their impact on core reactivity were examined. IPSN carried out physical core calculations, working independently or with support from CEA. One of these studies highlighted an initial sequence of 'heterogeneous dilution' events[927] involving boron in the core.

Discussions continued and in 1989, EDF, based on the results from probabilistic assessments of the sequences studied, identified a sequence with a significant

[927] These are events that could lead to insufficient boron concentrations in certain areas of the core.

probability of occurrence, i.e. a few 10^{-4} per reactor and per year. Consequently, the need to take additional measures against heterogeneous boron dilutions in the core was recognized by all stakeholders, in France and internationally. This sequence starts from an outage state, where the reactor coolant pumps are shut down, and corresponds to a transfer of pure water (or 'clear' water, i.e. non-borated) to the core when the pumps are restarted. Once this particular sequence was identified, EDF instructed its power plants to avoid any inflow of pure water in the reactor coolant system when the circulation pumps were shut down. In a second step, at the beginning of the 1990s, an automatic control device was installed to stop any inflow of pure water when the pumps were shut down. It is one of the components of what is called the 'anti-dilution protection system', which will be discussed below.

The event sequences studied in France were of course briefly presented to foreign partners through the various organizations involved, as part of bilateral relations and in international meetings organized by the OECD's Nuclear Energy Agency (NEA) or by the IAEA. Since the Three Mile Island accident, this has become standard practice in the nuclear industry, at least in the West. It is as important to alert other operators and nuclear safety organizations about an accident precursor, even if it is only theoretical, as it is to present real incidents. This is part of safety culture. The initial scepticism has dissipated, due in particular to probabilistic evaluations and later, to probabilistic safety assessments (PSAs).

35.1. Research and study of event sequences

As indicated above, following the Chernobyl accident, the manner in which reactivity insertions were postulated and handled in France was reviewed. The event sequences considered for the design of pressurized water reactors were reassessed along with their assumptions, and the possibility of other sequences potentially requiring additional measures was explored. Some of the operating conditions studied are included in the appendix.

To find the possible causes of a reactivity insertion accident, it is important to remember that in the pressurized water reactors operated in France, the core is under-moderated (see Chapter 5) and reactivity is controlled not only by the RCCAs that are inserted in certain fuel assemblies, but also by boron in the form of boric acid dissolved in the reactor coolant fluid. Postulated reactivity accidents can therefore be classified in three families:

- cooling accidents,
- accidents involving RCCA withdrawal or ejection,
- accidents involving decreased boron concentration in the reactor coolant fluid, called 'dilution accidents'.

The main studies on event sequences related to these three families are presented in the rest of this chapter. It should be noted that other exploratory sequence studies were conducted with a conservative focus; only a few of them will be mentioned below. These very low probability sequences assumed the occurrence of several failures (including reactor trip) or non-compliance with operational limits and conditions (such as the RCCA insertion limit). Studying them made it possible to specify the available margins relative to fuel damage or the time available to operators to take action before damage occurs.

35.1.1. Cooling accidents

The guillotine break of a main steam line at the steam generator outlet is considered the most severe accident of all the possible causes of sudden cooling of reactor coolant. It is thus included in the design-basis operating conditions for pressurized water reactors. The sudden increase in the steam flow rate following the break causes a rapid drop in pressure in the steam generators. The resulting increased temperature difference between the reactor coolant system and the secondary system rapidly cools the water in the reactor coolant system. Given the negative value of the moderator temperature neutron coefficient, this cooling effect introduces reactivity in the core. If the reactor is generating electricity, power temporarily increases until the protection system rapidly activates reactor trip, which interrupts the nuclear chain reactions. The insertion of RCCAs in the core thus creates a margin relative to critical conditions. This margin must be sufficient to mitigate the consequences of the cooling transient, which continues to introduce reactivity.

To limit cooling, the protection system also issues an order to close the isolation valves of the steam lines and the steam generator main feedwater lines. A shutdown signal for the reactor coolant pumps was also added to reactors in the French nuclear power plant fleet to reduce the cooling rate. However, cooling of the reactor coolant circulating in the RCS cold leg connected to the affected steam generator cannot be interrupted, since the break considered is upstream of the steam isolation valve. In this case, criticality conditions could be reached, causing a nuclear power excursion.

To limit the level of power reached, the protection system triggers automatic startup of the safety injection system, which supplies the necessary borated water for controlling reactivity after RCCA insertion as a result of reactor trip.

If an RCCA were to remain jammed despite reactor trip (an aggravating failure included in the accident study), a significant local power peak could occur in the area of the fuel assembly where the RCCA is jammed. The neutron feedback due to local heating of the fuel (Doppler effect) and the reactor coolant (moderator effect) would limit the amplitude of this peak.

A drop in RCS pressure also results from contraction of the water in the reactor coolant system due to cooling. These RCS pressure conditions and the power conditions in the fuel assembly induced by the jammed RCCA could damage the fuel rods due to the occurrence of a departure from nucleate boiling[928] and its consequences.

[928] See Section 5.6.

Certain reactors in the French nuclear power fleet (900 MWe reactors) have a tank of highly borated water and a safety injection pump that can send high-pressure borated water from this tank to the reactor coolant system. This makes it possible to automatically and rapidly restore a subcritical state in the core. For the 1300 MWe and 1450 MWe reactors, the safety injection system does not have high-pressure pumps, but rather medium-pressure pumps (this design change was adopted following the Three Mile Island accident). The borated water injection only occurs after a sufficient decrease in the reactor coolant system pressure, but to improve reactivity control, particularly in the event of a slower cooling transient that does not cause a significant pressure drop in the reactor coolant system, an 'automatic boration function' was designed to inject high-pressure borated water. However, this system is not taken into account in the safety studies. In all cases, the return to a stable and sustainable state with a sufficient subcriticality margin is only possible after operator action, notably to completely isolate water inflow to the affected steam generator (by closing the EFWS).

For the EPR, a dedicated safety system for controlling reactivity was specifically designed to automatically inject highly borated water at high pressure and a low flow rate, particularly in the event of a cooling accident. Moreover, the high number of RCCAs dedicated to reactor trip provides a significant margin with regard to critical conditions. Finally, the protection system issues an automatic and total isolation order for the feedwater of the affected steam generator (to isolate the MFWS and EFWS). In general, improvements introduced in the EPR design to control reactivity insertion transients caused by cooling make it possible to avoid the return of the reactor to a power state for all cooling incidents (caused by the most frequent initiating events) and certain cooling accidents. For steam-line rupture accidents that could nevertheless lead to a return to power (at most a few one hundredths of nominal power), these design measures guarantee that a subcritical state is reached in a completely automatic manner (without operator action).

After the Chernobyl accident, scenarios were studied that involved excessive cooling by the steam generators (with emptying of two, three, or four steam generators), with or without a jammed RCCA. Then extreme cases of steam line rupture were studied based on startup of the safety injection system with zero boron concentration or complete unavailability of this engineered safety feature. In all cases considered, the studies concluded that there is a risk of fuel damage if the RCCA with the greatest anti-reactivity worth remains jammed outside the core during reactor trip. According to the assessments conducted at the time, average power values significantly greater than 20% of nominal power could be reached (return to power). Given the high hot-spot factors[929] if all the RCCAs were to be inserted except for the one with the highest worth, departure from nucleate boiling could occur followed by damage to several fuel rods. However, the probabilities of these sequences were considered extremely low given the number and type of failures they assume.

[929] See Chapter 5, Section 5.2.

If all RCCAs drop into the core during reactor trip, the hot-spot factors remain low and the criteria relative to fuel integrity are still met. For the Flamanville 3 EPR, the safety analysis report includes a specific accident study involving simultaneous draining of two steam generators due to the complete double-ended guillotine break of two main steam lines, assumed to be caused by an aeroplane crash. The study shows that the reactor remains subcritical throughout the transient if there are no aggravating factors.

35.1.2. Incidents and accidents related to rod cluster control assemblies

The withdrawal of an RCCA from the core leads to reactivity insertion. Conversely, for pressurized water reactors, the insertion of an RCCA in the core always leads to a greater or lesser decrease of reactivity. Situations like the one that occurred in the Chernobyl RBMK reactor have not been identified, i.e. situations where, in certain configurations, the beginning of RCCA drop increases core reactivity.

▶ Incident involving control bank withdrawal

This incident, included in Category 2 of the design-basis operating conditions, could result from either a failure of the system for controlling the average RCS temperature or for controlling reactor power using the RCCAs, or a failure of the control rod system, or an operating error in cases where the operator must manually control the RCCAs when the reactor is generating electricity or when the reactor restart procedure is being monitored after an outage.

If <u>the reactor is generating electricity at full power</u> during the incident, the additional reactivity produced when the control banks are withdrawn is distributed throughout the core and nuclear power temporarily increases until the protection system causes reactor trip. Heat removal by the secondary side of the steam generators increases more slowly than the power released in the reactor coolant system; the result is an increase in the pressure and temperature of the reactor coolant. Given the increased neutron flux ('power ramp', but limited by neutron feedback) and the reactor coolant temperature, there is a risk of pellet-cladding interaction assisted by stress corrosion cracking[930], departure from nucleate boiling, and fuel melt in the centre of the pellets.

Whatever the reactor control mode, which differs according to which reactor series of the French nuclear power fleet is involved, the RCCA control system is designed to limit the reactivity insertion kinetics. The protection system is designed to activate reactor trip early enough to avoid any damage to the fuel rods.

[930] It should be recalled here (see Chapter 28) that pellet-cladding interaction assisted by stress corrosion cracking (SCC) may lead to cladding failure (loss of integrity), initiated on the inner surface of the cladding at the inter-pellet gaps. A power excursion causes the fuel to release corrosive fission products, such as iodine, cadmium, or caesium, in the space between the pellets and the cladding. SCC is likely to start in the interaction area, followed by propagation from the inside to the outside of the cladding, which could then lead to the transfer of fission products to the reactor coolant system water.

If the reactor is initially at zero power, in hot standby mode, or approaching critical conditions (during restart after an in-cycle outage), the additional reactivity from the withdrawal of one or more control banks initially inserted (depending on the instrumentation and control design and thus the reactor series design) may rapidly lead to reaching conditions of 'prompt criticality' from the beginning of RCCA withdrawal. Prompt criticality corresponds to a reactivity insertion of about 500 pcm. This leads to a very rapid excursion of nuclear power in spot locations in the lower part of the assemblies from which the RCCAs have started to be withdrawn. The amplitude of this power 'pulse' is limited only by the amplitude of the neutron feedback caused by heating of the fuel in very specific spots, then the fluid circulating between the assemblies. At the time of the power pulse, there is a risk of fuel melting and mechanical cladding failure due to the deformation caused by the thermal expansion of the pellets (pellet-cladding mechanical interaction). Directly afterwards, the potential risk is a departure of nucleate boiling before reactor trip occurs.

All possible control bank withdrawal situations have been postulated, taking into account the specific features of the reactor's RCCA control system design. The control bank composition, defined according to the reactor control mode, and the design of the associated control system (particularly the selection of banks that can be controlled simultaneously) guarantee that the fuel rods are not damaged in any of the possible withdrawal cases.

Rod cluster control assembly withdrawal accident

In contrast to the accident involving control bank withdrawal, the accident involving withdrawal of one RCCA (accident studied in Category 3 design-basis operating conditions) leads to a local increase of reactivity in the core. This kind of withdrawal can only occur in the following two cases:

- the operator deliberately raises an RCCA to correct real or assumed misalignment of the RCCA relative to its control bank,
- several electrical or mechanical failures occur simultaneously while the reactor is operating in automatic control mode.

This accident is only studied for a reactor operating at full power. The amplitude of reactivity insertion is limited compared to that corresponding to the uncontrolled withdrawal of control banks in this reactor state. However, the power increase being located in specific spots in the assemblies surrounding the withdrawn RCCA and the asymmetrical heating this increase causes in the fluid passing through the core may cause a risk of pellet-cladding interaction assisted by stress corrosion cracking, a risk of departure from nucleate boiling for certain fuel rods in this area, and a risk of fuel melting.

The definition of authorized insertion limits during full-power operation for the various control banks according to the reactor control mode, as well as the composition of the core loading pattern, make it possible to limit the withdrawal cases for which departure from nucleate boiling is a confirmed risk. In these cases, the design of the protection system guarantees reactor trip, aimed at preventing severe damage to the fuel rods if a high temperature is maintained. Studying the accident ensures that the number of rods that risk damage is sufficiently limited and that the temperature of the cladding and the time it is maintained at high temperature remain sufficiently limited, and that the same applies to any fuel melt in the centre of the pellets.

Following the accident at the Chernobyl nuclear power plant, the study of an RCCA withdrawal did not lead to additional investigations. This was because the consequences of more conservative scenarios, where it is assumed that the operator has failed to comply with the operating rules, were considered to be covered by studies of an accident involving an RCCA ejection (see next section). It was considered pertinent, however, to assess how long it would take to reach the maximum time to fuel rod damage if the reactor trip was not activated. This assessment showed that, in the event of an RCCA withdrawal leading to departure from nucleate boiling in a few rods in the core, combined with failure of reactor trip, the operator would have about 15 min to take action before any severe fuel damage would occur. But this risk was considered extremely low given the very low probability of this scenario.

▶ Accident involving a control RCCA ejection

Ejection of a control RCCA (accident studied in Category 4 design-basis operating conditions) could result from rupture of the control rod drive mechanism pressure boundary, which would create a pressure difference on the control rod drive shaft between the reactor coolant system pressure and the containment pressure. This ejection would result in very fast reactivity insertion that could lead to 'prompt criticality' conditions and thus a sudden increase in core power, accompanied by significant deformation of the radial distribution of power near the ejected RCCA. The local power increase would lead to a significant increase in the energy stored in the fuel pellets, whose expansion could lead to cladding failure (due to pellet-cladding mechanical interaction), departure from nucleate boiling and fuel melting, and finally more or less severe damage to certain fuel rods, depending on the neutron efficiency of the ejected RCCA. Cladding failure could lead to ejection of very hot fuel pellet fragments into the reactor coolant. The thermodynamic interaction between these fragments and the reactor coolant could have various consequences: vaporization, pressure increase, etc. that could lead to significant damage to the core or the reactor coolant system.

The criteria adopted concerning the control RCCA ejection accident in designing the reactors in the nuclear power plant fleet were initially taken from Regulatory Guide 1.77, prepared in 1974 by the US nuclear safety regulator (U.S. NRC). They aim to guarantee that fuel rod damage will be limited enough to sustain core cooling throughout the duration of the transient.

The criteria adopted (for moderate burnup rates) involve four parameters:

- maximum cladding temperature, which must remain below 1482°C (2700°F),
- maximum fuel enthalpy, which must be less than 200 cal/g,
- fraction of molten fuel, which must be less than 10%,

– number of rods where departure from nucleate boiling is liable to occur; this number must be less than 10% of the rods in the core.

Then, for high burnup rates, the criteria related to the variation of fuel enthalpy were investigated in numerous studies. Research work conducted using the CABRI experimental reactor is described briefly in Section 35.2. The criteria used by EDF for the maximum variation of fuel enthalpy are provided in this section.

The RCCA ejection accident is used to determine the operating limits relevant to control RCCA insertion when the reactor is in operation. These limits are defined for each control bank according to the reactor power level, so as to remain compliant with applicable safety criteria.

The fuel rod cladding materials in recent designs (presented in Section 28.2) have improved behaviour relative to the risk of cladding failure due to pellet-cladding interaction. This is because in normal operation, these materials are more resistant to corrosion, which can embrittle cladding for this type of transient.

35.1.3. Boron dilution accidents

Decreased boron concentration in the reactor coolant system water as a result of dilution may lead to significantly increased core reactivity.

Pure or ‘clear’ water can only enter the reactor coolant system from systems to which it is connected, from a leak through a reactor coolant system pressure boundary (a leak between the reactor coolant system and the secondary system through the steam generator tube bundles or a leak from the reactor coolant system during an outage), from the condensation of steam in certain reactor coolant system areas, or from water added to the reactor pool during a core refuelling outage, when the reactor coolant system no longer represents a closed boundary. Slow, homogeneous dilutions, which can be controlled by automatic control devices or operator actions, are unlike heterogeneous dilutions, which may lead to a rapid power excursion whose progress is governed by neutron feedback. Heterogeneous dilutions that may occur during certain accidents are called ‘inherent dilutions’ (see below).

A ‘precursor’ event involving the introduction of non-borated water in the reactor coolant system through a generator tube that had been cut open and was left incompletely obturated occurred in 1990 at the Blayais nuclear power plant (an event described in Section 23.1.2). Responding appropriately, the operators prevented the reactor from going critical.

Another precursor event involving the introduction of non-borated water in the reactor coolant system, at a slower rate, occurred in the Belleville nuclear power plant in 1991[931]. After a pressurizing check in preparation for a hydrotest on an accumulator filled with pure water for this purpose, an operability test was conducted to check the isolation foot valve on the accumulator. The accumulator was assumed to be empty,

[931] Event described in Section 23.1.2.

but it in fact contained 16 m^3 of non-borated water. Part of this water was drawn by gravity into the reactor core but did not cause a return to criticality. The non-borated water had in fact been mixed with the cooling system water and it flowed slowly because the accumulator vent was closed. In other circumstances, non-borated water could have entered the system more quickly and completely. Since this event, accumulator hydrotests are performed using borated water.

▶ Homogeneous dilution accident

The possible causes of homogeneous dilution are as follows:

- operator error in reading the boron concentration in the reactor coolant and in calculating the flow rates of water and boron to be injected into the reactor coolant system, or in calculating the volume of water to be injected in the system, or an error in the water volume displayed,
- failure of a component that belongs to one of the systems connected to the reactor coolant system,
- failure of the boron concentration adjustment control system in the reactor coolant system,
- leaks on an exchanger belonging to a system connected to the reactor coolant system.

The corresponding reactivity insertions are very low, and are significantly lower than the insertions that could lead to a rapid power excursion.

After the Chernobyl accident, the study of the homogeneous dilution transient, included in Category 2 operating conditions, was extended by assuming that no reactor trip was triggered and no operator action was taken. Studies showed that the gradual increase in reactivity would heat the reactor coolant, causing a decrease in reactivity by evaporation (the temperature coefficient of the moderator is negative). The reactor coolant system would gradually be drained by the pressurizer valves. However, the time to core melt would remain high.

▶ Heterogeneous dilution accident

The possibility of heterogeneous dilution was identified during analysis after the Chernobyl accident. The theoretical scenario adopted was as follows:

- a non-borated water ‘plug’ forms in a reactor coolant system loop (reactor coolant pumps shut down),
- the reactor coolant pump is restarted for that loop,
- the non-borated water plug is sent into the core,
- the core reaches criticality very quickly, adding a high amount of energy to the hottest fuel pellets,
- these pellets burst into very fine fragments and are dispersed,

- these very hot fragments interact with the coolant, which has not had time to boil on contact with the cladding,
- given the significant heat exchange surface area, a steam explosion occurs as the fuel interacts with the coolant,
- this leads to a reactor coolant pressure transient that depends on the number of burst pellets,
- this in turn leads to loss of integrity in the reactor coolant system if the pressure transient is high enough, and projectiles may be created as a result,
- these projectiles lead to a containment failure.

In this scenario, the risk of cladding burst and fuel fragment dispersion implies particularly high energy deposition and leads to a steam explosion. The effects of the explosion are more severe than boiling on contact with cladding since the heat exchange area involved represents a quite different scale.

The studies of this scenario were performed using conservative assumptions, given the uncertainty associated with the postulated phenomena. In particular, the possibilities of 'erosion' of the water plug while it forms were not considered. This phenomenon can nonetheless significantly limit the degree of danger engendered by the accident. EDF did, however, explore this phenomenon as part of experimental thermal-hydraulic studies first performed with the BORA-BORA experimental mock-up, which is representative of a 900 MWe reactor vessel at 1/5 scale. Later the studies were performed internationally using the PKL experimental loop[932] operated in Germany (in Erlangen) by Areva. This loop represents the reactor coolant and secondary systems of a KONVOI pressurized water reactor at a reduced scale (see Figure 35.1). Numerical simulations based on the test results were also conducted.

The above scenario corresponds to the alpha mode as defined in the Rasmussen report (WASH-1400, see Chapter 17), and could lead to releases corresponding to the S1 source term, in terms of their order of magnitude.

Based on the theoretical scenario, plausible sequences of events were sought that could lead to this type of accident so that additional preventive measures could be taken as necessary. Any action to mitigate the consequences would be ineffective given the duration of the phenomenon, about one second.

Based on physics studies, systematically looking for event sequences highlighted a sequence whose estimated probability was close to 10^{-4} per reactor and per year (already mentioned in the introduction to this chapter), before the implementation of corrective actions. The event sequence is as follows:

[932] This involved the PKL-1 (2004-2007), PKL-2 (2008-2011), and PKL-3 (2012-2016) programmes conducted by the OECD/NEA, in cooperation with IRSN. Aspects other than transfers of non-borated water into the core were also studied.

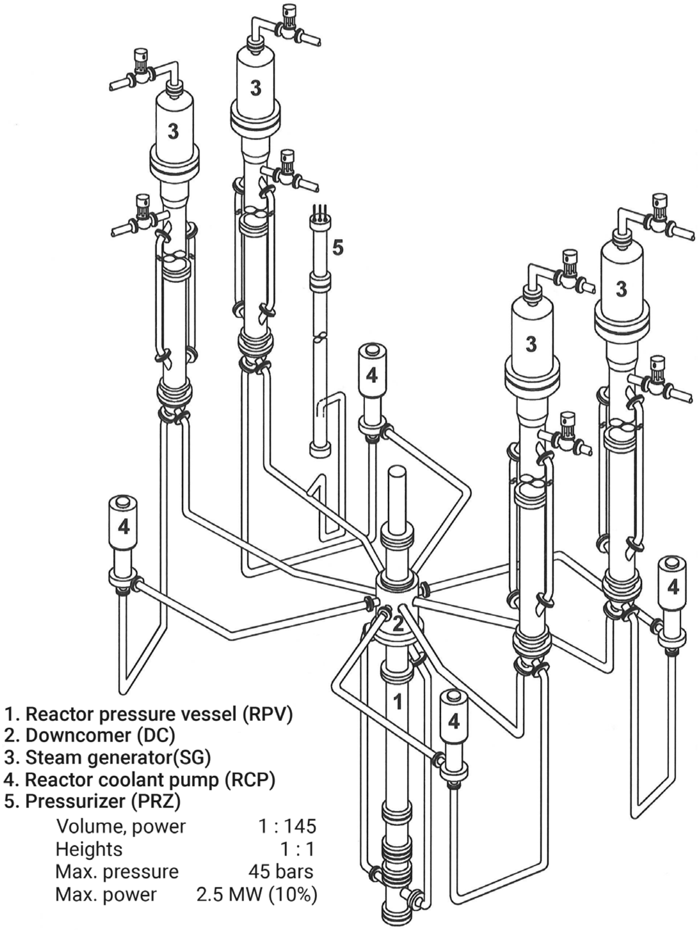


Figure 35.1. The PKL experimental loop (diagram from Main Benefits from 30 Years of Joint Projects in Nuclear Safety, OECD/Nuclear Safety, 2012).

- the reactor is in hot shutdown, at the start of the cycle (when the core is the most 'reactive');
- a dilution of boric acid is underway to reach criticality with a boron concentration of about 1000 ppm[933]; the dilution operation, starting with a boron concentration of 2000 ppm, necessary after shutdown, lasts about five hours;
- during dilution, the main off-site power supply fails, causing the reactor coolant pumps to shut down;
- it is assumed that natural water circulation in the reactor coolant system cannot be established or is blocked due to low residual power;

[933] See Section 5.6.

- the charging pumps of the chemical and volume control system (CVCS) and the demineralized water system (REA – water and boron makeup) are automatically resupplied by the auxiliary power supply without any operator action. Dilution thus continues. The reactor coolant system in which the non-borated water arrives via the charging line fills in about 15 min. Non-borated water may also accumulate at the bottom of the vessel by overflow;
- the reactor coolant pump of the loop that ensures normal water spraying in the pressurizer is then energized by the auxiliary power line or, when power is restored, by the main power line; it is returned to service according to the operating procedure. For the paired 900 MWe units and for all P4 1300 MWe units, this reactor coolant pump is the pump of the loop that the charging line, used for introducing non-borated water, feeds into;
- a non-borated water 'plug' is then transferred into the core.

This type of water plug would cause a return to criticality if it introduced a plug of more than 1 m^3 of clear, cold water in the core, for any reactor operating state. Taking into account fluid diffusion and mixing in the vessel, it was then determined that the admissible maximum volume of a non-borated water plug formed in the reactor coolant system would be 3 m^3. Other cases were studied: normal shutdown state with the residual heat removal system (RHRS) connected to the reactor coolant system, and in the event of maintenance or a refuelling outage. If the boron concentration in the reactor coolant system is at least equal to 2000 ppm and if the subcriticality of the reactor core is greater than 5000 pcm, the admissible maximum volume of the plug was estimated at 5 m^3.

As indicated above, once these scenarios were identified, EDF asked the power plant operators to ensure that all dilution was stopped if a reactor coolant pump associated with the charging line was shut down and to check, before restarting this pump, that no dilution operation had been performed. The minimum subcriticality (negative reactivity) required in normal cold and hot shutdown states[934] was increased from 1000 to 2000 pcm to guarantee that the reactor could not become 'prompt critical' during the introduction of a non-borated water plug. Moreover, in 1990, EDF studied and then installed in the reactors an automatic control function that transforms the dilution order into an action that sends borated water from the refuelling water storage tank (RWST, which contains water with 2000 ppm of boron) if a reactor coolant pump shuts down during dilution in a hot shutdown state. This measure, of which the 'initial' principle (a modification was made later, described in Section 35.1.4) is shown in Figure 35.2, significantly reduced the probability of this scenario by a factor of about 100. These elements were all brought together to form the anti-dilution protection system.

In addition, nuclear power plant personnel was made aware of the criticality accident risk in this case.

[934] For outage states with an 'open vessel' (outage for core refuelling or maintenance), the criticality deviation must be at least 2000 pcm, taking into account all the RCCAs raised with the vessel head (see Section 5.6).

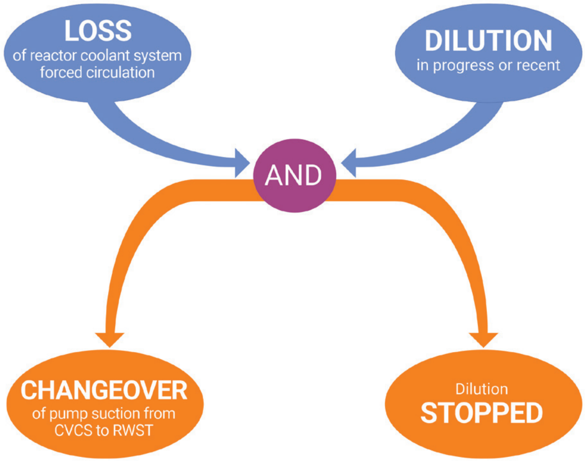

LOSS
of reactor coolant system forced circulation
DILUTION
in progress or recent
AND
CHANGEOVER
of pump suction from CVCS to RWST
Dilution
STOPPED

Figure 35.2. The initial principle of the automatic control function implemented in the anti-dilution protection system. IRSN.

Later, in 2005, when a safety review was performed[935], IRSN considered that the heterogeneous dilution scenarios that could result from an internal leak in the exchanger of the reactor coolant pump standstill seal system should be studied. The Level 1 probabilistic safety assessments conducted by the Institute showed that this heterogeneous dilution scenario was one of the predominant scenarios leading to core melt (core melt probability of about 2 × 10^{-7} per reactor and per year). This type of leak would introduce non-borated water from the component cooling water system (CCWS) of the exchanger in the CVCS then in the reactor coolant system by injecting water into the seals of the reactor coolant pumps. During maintenance or core refuelling outages, since the reactor coolant pumps are shut down, this non-borated cold water could accumulate due to density in the reactor coolant system U-legs, thus forming a non-borated water plug. During the transient to the shutdown state with cooling by the RHRS, the operator starts one of the reactor coolant pumps. This would then cause the non-borated water plug to be transferred to the core. The anti-dilution protection system was not operational in cold shutdown states and thus did not cover this dilution scenario.

EDF then conducted studies on the transfer of a non-borated water plug to the reactor core to demonstrate that there was no risk of a return to criticality in the possible scenarios involving dilution through the reactor coolant pump standstill seal system (CEPP) system. It also studied equipment and operating measures that could be implemented to eliminate this dilution scenario or significantly reduce its probability.

These studies ultimately led to equipment changes designed to detect any leaks in the CEPP exchanger before startup of the first reactor coolant pump, as part of

[935] Associated with the third ten-yearly 900 MWe reactor outage.

general studies associated with the fourth ten-yearly 900 MWe reactor outage. The principle of this change is based on monitoring the sodium concentration in the CVCS upstream and downstream of the CEPP exchanger. The sodium concentration is high in the CCWS (about 100 ppm) and low in the reactor coolant system (a few tens of ppb). A difference in sodium concentration in the CVCS upstream and downstream of the exchanger that is greater than a defined threshold would indicate a leak and would lead to prohibiting startup of the reactor coolant pumps. Samples are taken by an operator, with the reactor in the shutdown state and RHRS connected, about 8 h before the first reactor coolant pump is started.

For the reactors of other series (1300 MWe and N4), EDF presented a demonstration based on 3D numerical thermal-hydraulic simulations. According to the results obtained, the core remains subcritical during the scenario with a leak in the CEPP system.

▶ Inherent heterogeneous dilution accident

An inherent dilution is any heterogeneous dilution that could occur during or following certain accidents. The various scenarios involved are presented below.

In the case of a reactor coolant system break, there is vaporization of borated water at the core outlet. During this vaporization, boron is not entrained in the vapour phase. Part of the produced vapour may condense in the steam generators, forming non-borated water plugs in the crossover legs of the reactor coolant system and the steam generators. These water plugs may enter the flow in the reactor coolant system when natural circulation of the water (in thermosiphon mode) begins. One of the difficulties of the corresponding studies resides in the choice of assumptions concerning the volume and number of plugs to be postulated, and in the kinetics of the return to natural circulation (number of loops where return to natural circulation occurs and flow rate changes). For this purpose, EDF used the results of tests in the PKL experimental loop mentioned above, but the representativeness of these results relative to the French nuclear power plant fleet is debatable. Consequently, for the Flamanville 3 EPR and for early reactors, EDF conducted robustness studies on the size and number of plugs and on their speed of insertion in the core. These studies showed that the simultaneous transfer of several 25 m^3 plugs (maximum possible size) leads to prompt criticality but does not have unacceptable consequences for the fuel, given the low enthalpy deposition in the fuel.

In the event of a steam generator tube rupture, if the pressure on the secondary side of the affected steam generator were greater than the pressure on the reactor coolant system side, the non-borated water of the secondary system would be entrained to the core when the reactor coolant pump of the affected loop is restarted. This is referred to as ‘backfilling’ the reactor coolant system with water from the secondary system. EDF modified operating procedures to prohibit restarting the reactor coolant pump of the affected loop.

Finally, the PKL tests conducted in the 2000s brought to light a risk of inherent heterogeneous dilution in the reactor shutdown states with RHRS cooling. The 'simple' loss of the RHRS is liable to cause a switch to heat pipe conditions[936] in the steam generators and thus dilution of the boron entering the vessel. EDF continued to study this subject, analysing the PKL studies performed in 2018 for a three-loop reactor configuration. The first tests that highlighted the problem were conducted for a four-loop reactor configuration. The conclusions drawn by EDF will be sent to nuclear safety organizations at a later time.

35.1.4. Inserting a cold water plug in the core

The boron dilution scenarios presented above were based on a rapid decrease of boron concentration in the reactor coolant system at constant temperature. Further studies attempted to identify event sequences that could lead to transfer of water colder than that of the reactor coolant system into the reactor core; at a constant boron concentration, the decreased temperature of the core cooling water, initially at 297°C, leads to a significant introduction of reactivity (see Figure 35.3).

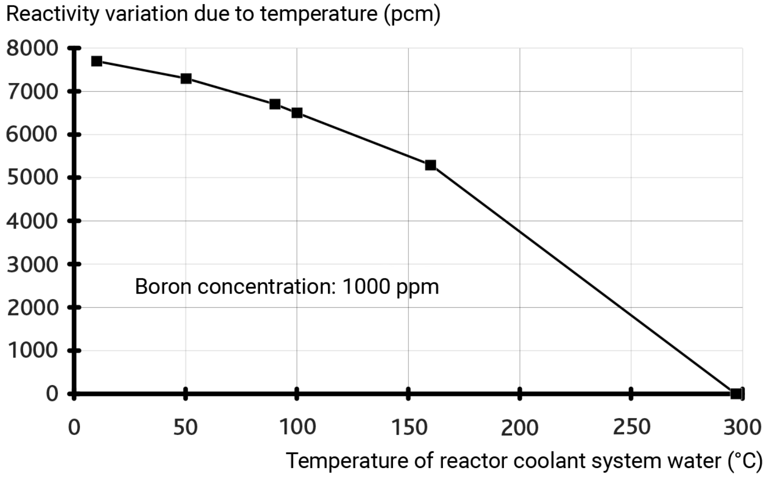


Figure 35.3. Overall effect of a temperature variation in the core water at shutdown. IRSN.

One of the possible sequences is similar to the scenario described for non-borated water plugs.

The hydrodynamic seals of the reactor coolant pumps are supplied with water from the chemical and volume control system to ensure they are sealed tight. This water has the same boron concentration as the water injected into the reactor coolant system by

[936] Heat transfer achieved through a fluid phase transition. The fluid is vaporized at a hot source (evaporator), then the vapour circulates to a cold source (condenser) where heat dissipation takes place.

the CVCS. By contrast, since it does not go through the regenerative heat exchangers that would bring it to the temperature of the reactor coolant system water before its insertion into one of the loops, the water sent to the seals is cold (about 40°C).

If a main electrical power supply failure occurs during hot shutdown of the reactor, water supply to the reactor coolant pump seals is maintained. Cold water could then fill the intermediate loops if residual heat is insufficient to maintain natural circulation in the reactor coolant system. When a reactor coolant pump starts up again, this mass of water, more or less mixed with water in the reactor coolant system, would be inserted in the core.

To counter the possible effects of this type of scenario, which seems to have a significant probability, in 1993 EDF decided to change one of the automatic anti-dilution protection signals. This change was implemented on the reactors. The injection of borated water from the refuelling water storage tank was activated by shutdown of the reactor coolant pumps, coinciding with insertion of non-borated water into the reactor coolant system. While the first signal was kept, the second is now generated from a calculation of core residual power to ensure that natural circulation in thermosiphon mode can be established (this calculation combines the core cooling time starting from shutdown with an assessment of the power level generated before this shutdown).

This new system (the 'final' anti-dilution protection function) still meets the objectives of preventing the insertion of a non-borated water plug, while being more general in scope.

35.2. Changes in criteria

As indicated above (see Section 35.1.2), the nuclear safety criteria (or technical acceptance criteria) with regard to fuel behaviour that were adopted for reactivity accidents studied as Category 4 operating conditions were established in the 1970s based on tests performed in the USA.

Concerning maximum admissible fuel enthalpy, the value initially set in the 1974 Regulatory Guide 1.77 was 280 cal/g for UO_2 fuel. However, a value of 200 cal/g for UO_2 fuel irradiated to 33 GWd/tU (average value per assembly) was then adopted in France. These limits aim to guarantee that hot or molten fuel fragments are not dispersed in the reactor coolant system, and therefore contribute to ensuring that core cooling capacity is maintained.

In the early 1990s, the Chernobyl nuclear power plant accident, together with the gradual increase in fuel assembly burnup rates targeted by nuclear operators, raised the question of the validity of the criteria that been established for moderate burnup rates.

Research programmes were initiated in this area, mainly in Japan and France, with 12 tests performed by IPSN from 1993 to 1998 using the liquid sodium loop which, at that time, was featured on the CABRI research reactor (PWR-Na tests). These programmes aimed to improve understanding of the phenomena occurring after the first hundreds of milliseconds that could lead to the failure of fuel rod cladding through pellet-cladding mechanical interaction and to the ejection of hot fuel fragments in the reactor coolant system. This ejection could cause cooling difficulties in the reactor core and jeopardize the robustness of the reactor coolant system. The PWR-Na tests were performed on rod sections from nuclear power plants with local burnup rates between 28 and 76 GWd/tHM (tonne of heavy metal, i.e. UO_2 or MOX). MOX fuel was used in four of these tests.

In France, in the 2000s, a proposal by EDF was discussed that aimed to define a 'decoupling domain' for high burnup rates (above a value set to 47 GWd/tU on average per assembly). This involved UO_2 and MOX fuels as well as the various additional cladding materials then in use[937] (the criteria cited above in Section 35.1.2 also had to be satisfied, including a maximum enthalpy of 200 cal/g). The decoupling domain aimed to guarantee that cladding failure would not occur in the event of a reactivity accident, taking into account cladding corrosion in normal operation. Thus, specific new criteria[938] were adopted by EDF (and approved by ASN in 2011, but with additional requests, particularly concerning the intermediate burnup rates and RCCA ejection transients initiated at power).

However, a comprehensive review (by EDF, IRSN, and the Advisory Committee for Reactors) of the nuclear safety requirements and criteria for fuel resistance was performed more recently, in 2017, to take into account new knowledge. For burnup rates above 33 GWd/tU, EDF proposed new criteria[939] on enthalpy variation and power pulse duration, ensuring that cladding failure due to pellet-cladding mechanical interaction would not occur, taking into account the performance of various types of cladding[940] with regard to corrosion (particularly the absorption of hydrogen in normal operation). These criteria are applicable to RCCA ejection transients starting at zero power, but not directly to those that could occur at power. For the latter transients, EDF developed a calculation approach to guarantee that cladding failure due to pellet-cladding mechanical interaction would be avoided. It is interesting to note that, within the regulatory limit of 52 GWd/tU (on average per assembly), these criteria also

[937] Namely M5®, Zirlo™, and Optimized Zirlo™ (see Chapter 28). It should be mentioned that for Zircaloy-4 (which has not been used for new assemblies loaded in reactors since 2016), the decoupling domain is not applicable and a specific demonstration was provided by EDF in 2014 to take into account spalling of this cladding in normal operation (in particular, implementation of compensatory measures in operation).

[938] Maximum enthalpy variation of 57 cal/g, transient time at mid-height of the 30-ms pulse, oxidized thickness less than 108 μm, and cladding temperature less than 700°C.

[939] For burnup rates greater than 47 GWd/tU, these new criteria replace the decoupling domain defined earlier.

[940] Thus, EDF has adopted an enthalpy variation limited to a little less than 80 cal/g and a power pulse duration, calculated at peak mid-height, of at least 30 ms for UO_2 fuel with Zirlo™ cladding, an enthalpy variation limited to 150 cal/g for UO_2 fuel with M5® cladding (with a pulse duration at peak mid-height of at least 5 ms), and an enthalpy variation limited to 100 cal/g and a pulse duration at peak mid-height of at least 30 ms for MOX fuel with M5® cladding. These criteria are valid for the specified maximum hydrogen contents in the cladding.

guarantee that fuel will not be dispersed in the reactor coolant system in the event of cladding burst in a departure from nucleate boiling situation.

Moreover (for all the RCCA ejection cases), in the absence of cladding ballooning, EDF has proposed to supplement the maximum cladding temperature criterion (1482°C) by placing a limit on the equivalent cladding oxidation rate (ECR[941]), to take into account the time during which cladding is subjected to high temperatures. These criteria would guarantee that failure would not occur on cladding embrittled by high-temperature oxidation during rewetting of the cladding. If cladding ballooning has been found, the criterion applicable to LOCA transients in terms of ECR, a function of the hydrogen content of the cladding, is used.

Finally, fuel melt (limited to 10% of the volume fraction) must be ruled out at the periphery of the fuel pellets and the number of rods liable to undergo departure from nucleate boiling must not exceed 10% of the core rods.

To study phenomena related to the behaviour of fuel rods that could, after the power peak, undergo departure from nucleate boiling (cladding drying and bursting) and to examine the potential consequences of fuel dispersion in the coolant after cladding failure that could impact the reactor structures in terms of a pressure wave, in the 2000s IPSN initiated a new experimental programme entitled the Cabri International Programme (CIP) led by the OECD/NEA and in partnership with EDF and a number of nuclear safety and industrial organizations from other countries (including EPRI, U.S. NRC, JAEA, GRS, etc.). This new programme covered the various cladding materials used (M5®, Zirlo™, Optimized Zirlo™, etc.). It was accompanied by an overhaul of the CABRI facility, with the installation of a new pressurized water loop (replacing the sodium loop of the PWR-Na programme; see Figure 35.4) for conducting tests in conditions representative of those that fuel rods in pressurized water reactors would be subject to during a reactivity accident. The first test (which also established loop qualification) took place in 2018.

35.3. The case of outage states

The purpose of a nuclear reactor is to generate electricity while the facility is operating at power, thus in a state where neutron physics are said to be ‘critical’ (i.e. where the nuclear chain reaction is sustained). When the reactor is shut down, however, the critical state must be avoided.

A severe criticality accident occurred on 30 September 1999 in Japan in a nuclear fuel fabrication workshop at Tokai-Mura as uranium oxide powder enriched in uranium-235 was being dissolved in nitric acid to obtain uranyl nitrate. The operators filled a tank with 16.6 kg of uranium, even though the limit mass was set at 2.4 kg. A blue flash characteristic of a criticality accident was observed (Cherenkov effect). Of those on the site, 136 people were irradiated, three of them seriously.

[941] Equivalent Cladding Reacted.

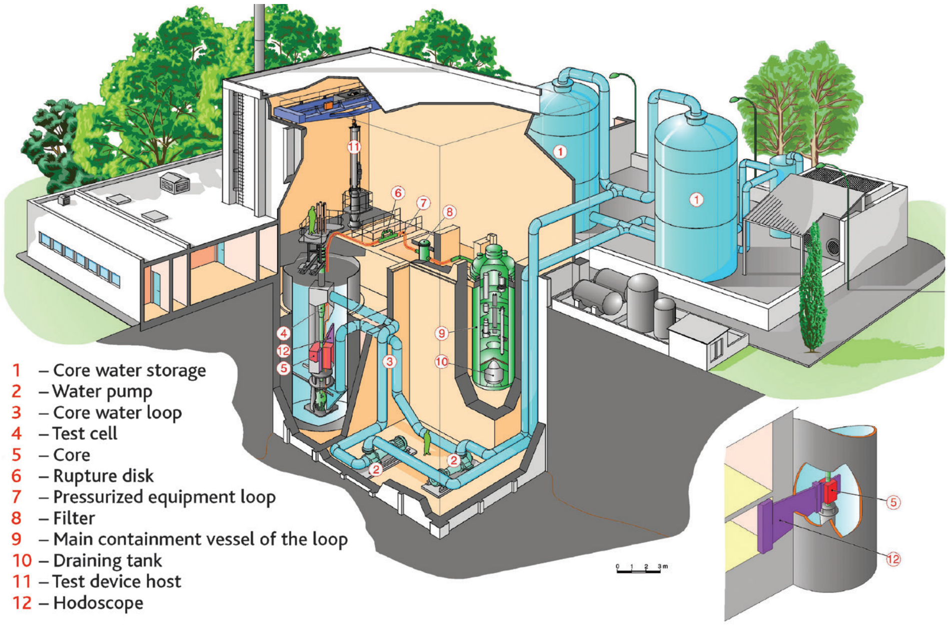


Figure 35.4. View of the CABRI reactor and the pressurized water loop facility. IRSN.

This accident led EDF to conduct a technical review of all the criticality risks associated with reactor operation in the French nuclear power plant fleet. This, in turn, led to the creation of criticality reference documentation that describes the conditions for taking into account the criticality risk for activities in the fuel building and the reactor building, in states where the reactor vessel is open. This documentation also stipulates the requirements for conducting criticality studies (acceptance criteria, rules for studies of normal and accident situations, methods, uncertainties, simulation code qualification, etc.).

The list of situations identified as liable to present a criticality risk is as follows:

– for the fuel building:

  - an accidental immersion of the dry storage rack for fresh fuel assemblies in non-borated water or in a non-borated water mist,
  - an accidental decrease of the boron concentration in the pool water,
  - an abnormal geometrical configuration for storing fuel assemblies (the assemblies are assumed to be intact),
  - an accidental dispersion of fuel rods or fuel pellets,
  - dropping a transport cask,
  - storage of a fuel assembly in an inappropriate area (assuming there are different storage areas);

– for the reactor building:

  - an accidental decrease of the boron concentration in the reactor pool water,
  - an accidental withdrawal of RCCAs when the vessel head is lifted,
  - fuel loading in a configuration non-compliant with the reactor core loading pattern.

The absence of criticality accident risk is demonstrated by substantiating the existence of an overall subcriticality margin of 2000 pcm (*keff* < 0.98) in the situations mentioned above or by implementing at least two independent and reliable 'lines of defence'[942] to substantiate that the criticality risk can be ruled out.

A reactor is equipped with instruments used to detect an increase in neutron flux. These detectors ('source range channel', SRC[943]), placed around the vessel, measure the neutrons outside the vessel. If this neutron count increases, the neutron flux inside the reactor core is also increasing. When the increase in neutron flux exceeds a threshold, an alarm alerts the operator of an unexpected variation in neutron flux. This alarm must occur early enough to leave operators the time to take action before a criticality accident occurs. The operators then implement the actions defined in procedures. However, these measures may not be as effective during core loading or unloading phases. That is why an event that occurred in 2001 during core refuelling at a reactor of the Dampierre-en-Burly nuclear power plant was considered as a precursor event for a criticality accident.

▶ Event that occurred in 2001 during core refuelling at Unit 4 of the Dampierre-en-Burly nuclear power plant

In 2001, during core refuelling at Unit 4 of the Dampierre-en-Burly nuclear power plant, a fuel assembly loading error offset the positioning of 113 fuel assemblies (see Figure 35.5).

The offset assemblies were only detected by the operators toward the end of loading (when the 135th assembly of 138 was loaded).

The studies conducted by EDF showed that, in more conservative conditions (loading all-new assemblies with a boron concentration at the minimum value required by operational limits and conditions, i.e. 2000 ppm instead of the 2345 ppm concentration present during loading at Dampierre 4), the error would have caused the reactor to reach criticality when the 121st assembly was loaded.

[942] Technical or organizational provisions that constitute a defensive measure against a postulated phenomenon.

[943] Neutron flux chambers are described in Section 5.6.

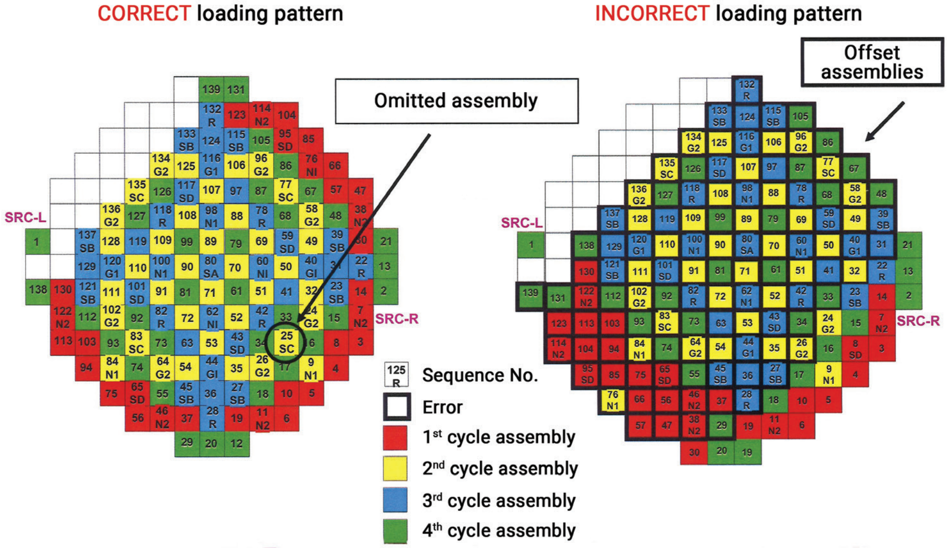


Figure 35.5. Dampierre Unit 4 core loading error. IRSN.

The event revealed that both the organizational and technical measures taken with regard to the risks of criticality accidents were insufficient. Organizationally, the following shortcomings were noted:

- insufficient communication between the operators in the reactor building and those in the fuel building,
- lack of full compliance with procedures.

These points were corrected.

Technically, calculations performed after the fact highlighted a significant increase in neutron flux that the SRCs had not detected. This lack of detection by the SRCs was explained by EDF in 2005: the 'field of vision' of the SRCs, situated outside the vessel, is relatively limited. If, due to an accident, the number of neutrons strongly increases in certain core areas, the SRCs may not be sensitive enough to detect this increase in these areas. This is what happened during the loading error at Dampierre 4.

Measures were taken to compensate for this neutron flux monitoring failure. In 2003, EDF took organizational measures to prevent incorrect positioning of the fuel assemblies. It was also demonstrated that a permutation of fuel assemblies could not lead to criticality.

In addition, EDF demonstrated in 2003 that the boron concentration in the reactor coolant system was sufficient to avoid a criticality accident due to RCCA withdrawal when the vessel head was lifted.

Finally, in 2005 EDF decided to use the existing device for continuous boron concentration measurement in the reactor coolant system (the nuclear sampling system, NSS), referred to as a 'boron meter', for early detection of any decrease in boron concentration in the reactor coolant system water. More recently, EDF decided to install another boron meter with a different design on another system (the CVCS), allowing direct, rapid measurement of the boron concentration in the reactor coolant system water. This second system[944] is now used in the safety demonstration for the outage states where all RCCAs are inserted (outage for refuelling only, maintenance outage, and normal shutdown with connection to the residual heat removal system when all the reactor coolant pumps are shut down).

In normal shutdown in RHRS states where the reactor coolant pumps are operating as in a normal shutdown with residual heat removal ensured by the steam generators, some control banks must be withdrawn. The safety demonstration is thus based on a reactor trip activated when the 'source level high flux' threshold is reached (immediately after critical conditions have been reached).

Studies on reactivity insertion incidents and accidents in these outage states show that, given the subcriticality margin guaranteed by the inserted control banks and the minimum required boron concentration, the impact of the reactor trip makes it possible to avoid prompt criticality and ensure the return to a subcritical state.

35.4. Regulations

The 'criticality baseline' was defined by EDF in application of Article 45 of the French Order of 31 December 1999 which stipulates that:

"Nuclear facilities containing fissile materials shall be designed, built, and operated to avoid any criticality accidents. More specifically:

- a criticality accident shall never result from a single anomaly: failure of a component or function, human error (such as failure to comply with instructions), an accident situation (such as fire) [...];
- if a criticality accident may result from the simultaneous occurrence of two anomalies, it shall then be demonstrated that:
  - the two anomalies are strictly independent;
  - the probability of occurrence of each one of the two anomalies is sufficiently low;
  - each anomaly can be detected using appropriate and reliable monitoring systems within a time frame that allows the necessary operations to be performed."

[944] This is a boron meter that measures neutron attenuation. It is non-intrusive and is installed around the CVCS letdown line.

These provisions were taken from fundamental safety rule RFS I.3-c, applicable since 1984, regarding the prevention of criticality risks in basic nuclear installations that do not include nuclear reactors.

Article 3.4.II of the INB Order of 7 February 2012 now stipulates that: "Regarding control of nuclear chain reactions, the operator shall demonstrate that the measures taken prevent the risk of criticality when criticality is not desired." This order, in application since 1 July 2013, updates the order of 31 December 1999, which has been repealed.

In 2011, ASN, in cooperation with IRSN, set out to revise fundamental safety rule RFS I.3-c, extending its scope to include power reactors. In 2014, this revision led to Decision No. 2014-DC-0462 of 7 October 2014 "relative to controlling the risk of criticality in basic nuclear installations." For nuclear reactors, this decision applies to the outage phases for fuelling or refuelling or for maintenance, and to the fuel storage pool.

Issued in 2017, ASN Guide No. 22, relevant to pressurized water reactor design, recommends (paragraph 3.3.1.2.3) that, for design-basis operating conditions, "the measures taken for controlling nuclear chain reactions aim to avoid reaching critical conditions in reactor outage situations" (when a single initiating event occurs, such as reactivity insertion). In paragraph 6.1, it recommends "ensuring that critical conditions are not unintentionally reached in states where the vessel is closed and the reactor is shut down in normal operation."

Appendix

Operating conditions adopted for pressurized water reactors in the French nuclear power plant fleet characterized by the insertion of reactivity in the reactor core

Category 2: Incidents of average frequency

- Uncontrolled withdrawal of control banks, reactor at power or at zero power (in hot standby, subcritical approach, or outage state)
- Uncontrolled dilution of boric acid
- Spurious opening of a secondary system valve

Category 3: Very infrequent accidents

- Withdrawal of a control RCCA at full power
- Small break in a secondary system line containing water or steam

Category 4: Significant postulated accidents

- Control RCCA ejection
- Complete rupture of a steam generator tube
- Significant rupture in a secondary system line containing water or steam

Chapter 36

The Reactor Accident at the Fukushima Daiichi Nuclear Power Plant and Lessons Learned in France

On 11 March 2011, a major earthquake (magnitude 9) struck Japan, with its epicentre 80 km to the east of Honshu Island; it was followed by a tsunami. The earthquake and the resulting tsunami severely affected the Tohoku region of Japan, with serious consequences for the population[945], the land and marine environment, and infrastructure.

One of the major consequences will have repercussions on nuclear safety for many years: these natural events devastated the site of the Fukushima Daiichi nuclear power plant, causing core melt in three nuclear reactors and prolonged loss of cooling in the spent fuel pools. Explosions occurred in reactor buildings. Very significant amounts of radioactive substances were released into the environment. The accident was classified Level 7 on the INES scale.

[945] Tsunami casualties totalled over 20,000 people dead or missing, mainly in the Miyagi, Iwate and Fukushima prefectures.

36.1. Reactor units at the Fukushima Daiichi nuclear power plant

The Fukushima Daiichi site is located on the seashore 250 km north-east of Tokyo. In 2011, it comprised six boiling water nuclear power reactor units (BWR) with power outputs ranging from 460 to 1100 MWe, commissioned between 1971 and 1979 and operated by the electrical utility TEPCO (Tokyo Electric Power Company) (see Figure 36.1).

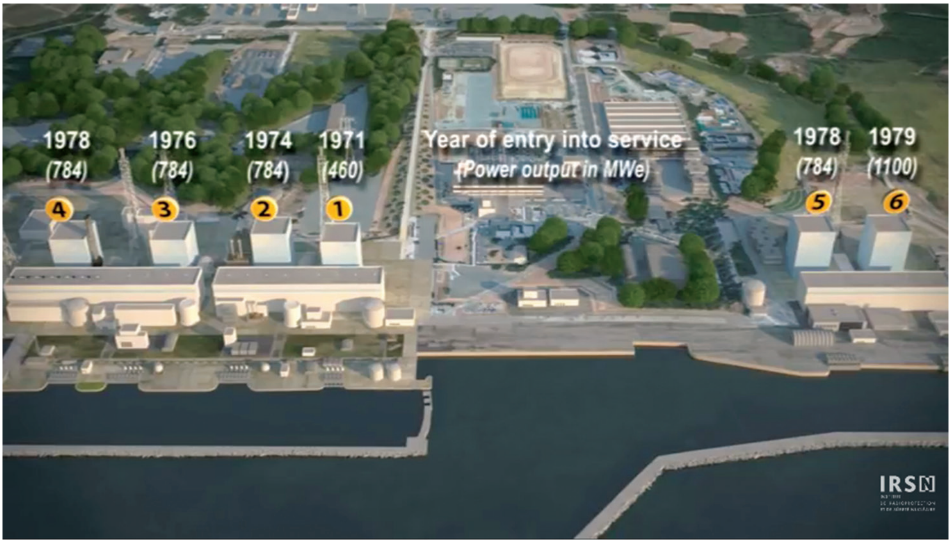


Figure 36.1. The site and reactor units of the Fukushima Daiichi nuclear power plant. Source: Analysis by IRSN of the Fukushima Daiichi Nuclear Accident of March 2011 (video), Jean-Yves Pipaud, Patrick Barra, Epsim/IRSN Media Library.

36.1.1. General operation of a boiling water reactor

Boiling water reactors (BWR) (see Figure 36.2) differ from pressurized water reactors (PWR) in that the water is vaporized as it passes through the reactor core and the steam produced is conveyed directly to the turbine, with no intermediate system. After passing through the turbine, the condensed steam is returned to the core. The reactor vessel operates at a pressure of about 70 bars and steam temperature is about 300°C.

36.1.2. Containment

The containment of a boiling water reactor is very different from that of a pressurized water reactor. Moreover, there are several designs. Units 1 to 5 at the Fukushima Daiichi nuclear power plant have a Mark I-type containment[946] (Figure 36.3) which features:

[946] Unit 6, undamaged, has a Mark II-type containment: the truncated-cone-shaped drywell is made of steel-lined concrete in the reactor part, and is prolonged by a cylindrical wetwell (condensation chamber), also made of steel-lined concrete.

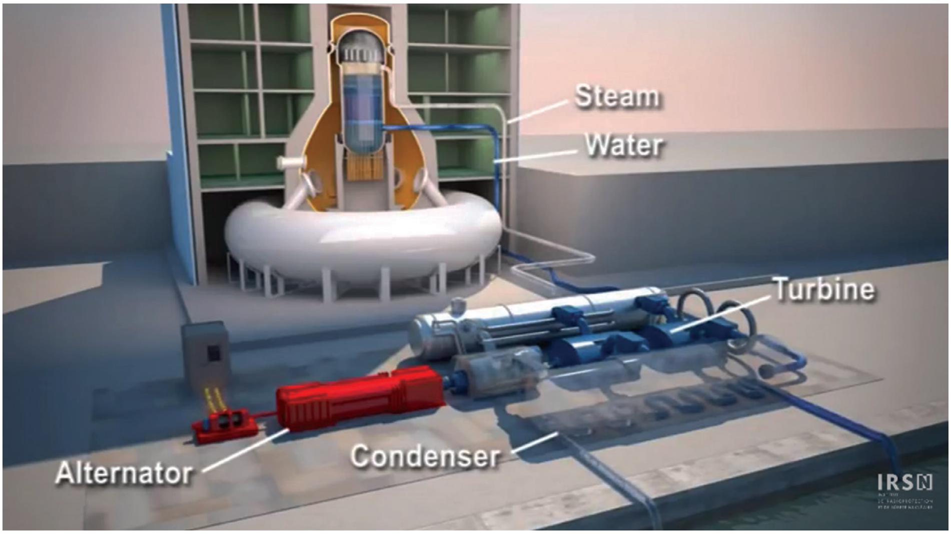


Figure 36.2. General view of a boiling water reactor (BWR) (Mark I-type reactor shown). Source: Analysis by IRSN of the Fukushima Daiichi Nuclear Accident of March 2011 (video), Jean-Yves Pipaud, Patrick Barra, Epsim/IRSN Media Library.

- a steel chamber, the drywell, shaped like a light bulb, which houses the reactor vessel; the drywell is filled with nitrogen, an inert gas;
- a toroidal steel condensation chamber, the wetwell, forming the bottom part of the containment; the wetwell contains water up to about half its height, forming a pressure suppression pool, with a nitrogen blanket above the water surface.

The wetwell has two essential functions:

- in the event of a pipe break that would cause a pressure increase in the drywell due to mixing of liquid water and released steam, the mixture would be conveyed through pipes from the drywell to the suppression pool, where it would be condensed by bubbling, thereby limiting the containment pressure increase;
- if the pressure in the reactor vessel needs to be limited, the wetwell can be used to remove water from the vessel through a pipe connecting it to the suppression pool.

In both cases, the suppression pool must be cooled: this is one of the functions of the residual heat removal system (RHRS).

If pressure in the containment becomes too high, it may be discharged out of the containment through valves on lines connected to the wetwell or the drywell.

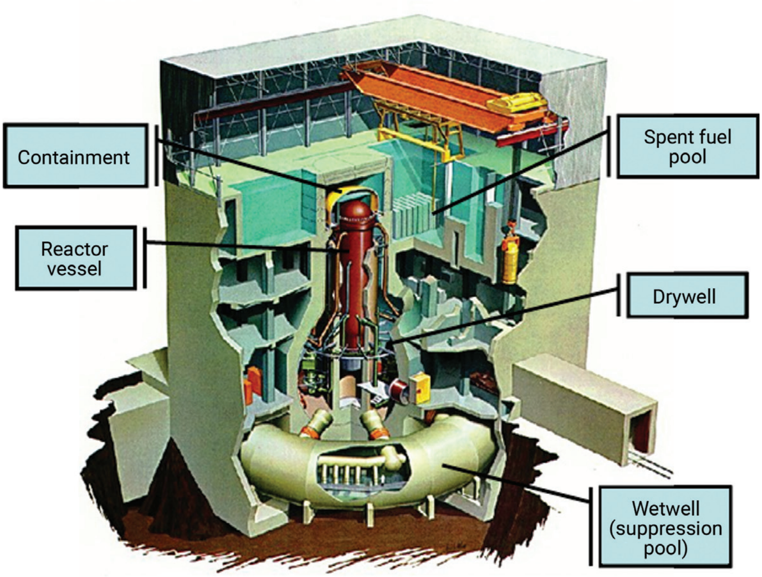


Figure 36.3. Containment of a Mark I-type boiling water reactor. Courtesy of the U.S. Nuclear Regulatory Commission.

The containment is housed in a concrete structure consisting of the reactor building. The reactor building itself is therefore not the containment of a boiling water reactor, as is the case for pressurized water reactors.

The reactor building also houses the spent fuel pool, located in the upper part.

36.1.3. Emergency cooling systems

The different units of the Fukushima Daiichi nuclear power plant have different emergency cooling systems (Figure 36.4). The discussion below concerns the three units in which core melt occurred during the accident.

▶ Units 2 and 3: the Reactor Core Isolation Cooling system (RCIC) and the High-Pressure Coolant Injection system (HPCI)

The RCIC is designed to remove residual heat from the reactor. A turbine-driven pump feeds water to the core from the condensate storage tank or, when this tank is empty, from the torus. The steam produced in the reactor vessel turns the turbine, which drives the pump.

The HPCI system is similar to the RCIC, but delivers a much higher water flow rate. It is designed to compensate for water losses if there is leakage from systems connected to the reactor vessel.

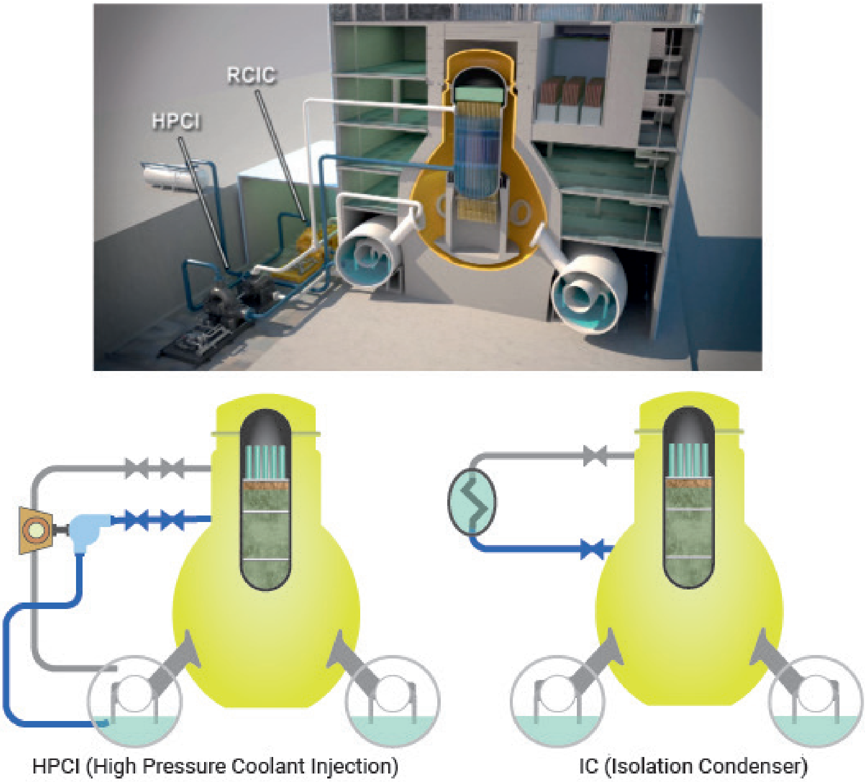


Figure 36.4. Schematic diagrams of the RCIC, HPCI and IC. Source: Analysis by IRSN of the Fukushima Daiichi Nuclear Accident of March 2011 (video), Jean-Yves Pipaud, Patrick Barra, Epsim/IRSN Media Library.

▶ Unit 1: the Isolation Condenser (IC) and the HPCI

Unit 1, the oldest, does not have reactor core isolation cooling (RCIC). In addition to high-pressure coolant injection (HPCI), it has an isolation condenser (IC), a system without a pump or turbine. The IC system has two redundant trains, each with a heat exchanger, that function using natural convection. The steam exiting from the core moves up naturally in the IC pipes, which pass through a large-capacity water tank where the steam condenses; the condensate returns to the reactor vessel by gravity. The water evaporating from the tank is discharged to the atmosphere outside the reactor building. The tank can be refilled from a tanker truck.

The IC, RCIC and HPCI are designed to maintain the appropriate liquid water level in the reactor. There are other cooling systems that are not discussed here because they were not able to function during the accident.

36.2. Sequence of events during the accident

On 11 March 2011, units 1, 2 and 3 were operating at full power; the core of Unit 4 had been unloaded to the spent fuel pool; units 5 and 6 were shut down.

At 14:46 local time, Japan was struck by a magnitude 9 earthquake that caused total loss of off-site power to the Fukushima Daiichi site. Units 1, 2 and 3 were tripped automatically by RCCA insertion into the core. The residual heat removal systems started up, powered by the emergency diesel generators.

Less than one hour after the earthquake, a tsunami struck: the site facilities were submerged by a series of waves. The most devastating, with a height of 1415 m above the mean sea level, was recorded at 15:42. This was almost 10 m higher than the dyke protecting the site (Figure 36.5).

The pumping stations of the six reactor units, located on a platform 4 m above the mean sea level, were severely damaged and the cooling pumps of the plant facilities were flooded, depriving the reactor units and their spent fuel pools of their normal cooling water sources. The water then penetrated into the nuclear island buildings, on a platform 10 m above the mean sea level, resulting in loss of the emergency diesel generators and the electrical switchboards.

The only emergency generator available for sustained use was the air-cooled generator of Unit 6, alternating its connection between Unit 5 and Unit 6. All of the other units on the site were in a situation of total loss of off-site and on-site power supplies and loss of ultimate heat sink.

Nevertheless, the batteries of Unit 3 were still operational after the tsunami. In contrast, the control rooms of units 1 and 2 did not have any lighting; the loss of their batteries resulted in the loss of crucial information on the state of the facilities, in particular the operating state of certain systems.

Lastly, the loss of electrical power led to loss of a large number of communication resources designed to provide information for the emergency response teams.

The significant events that, from the functional point of view, marked the development of the situation for each of the units 1 to 4 are described below. The extreme conditions in which the operators and the responding personnel had to take action must be borne in mind. In addition to the loss of means of information and telecommunications, the lack of preparation for such a situation, and consequently of written procedures and organization defined in advance, and the need to find equipment elsewhere, generally overwhelmed the emergency response teams. The dedication and the professional approach of the teams, their commitment, despite the aftershocks of the earthquake, the threat of more tsunamis and the increase in radiation levels, could not compensate for the low level of preparation in the face of the complexity of an accident of such magnitude, complexity aggravated by the large number of facilities affected, comprising the reactors and pools of several units. This resulted in difficulties – and sometimes errors – in the definition of priorities.

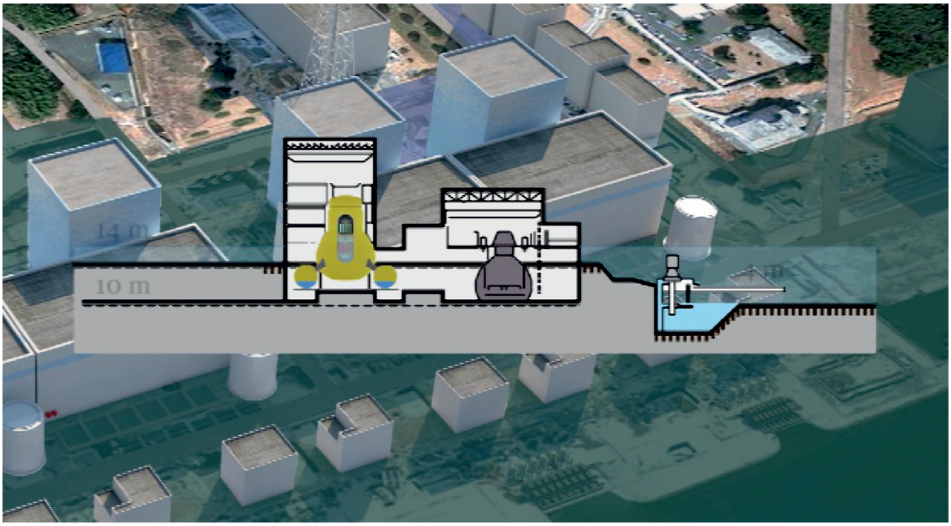


Figure 36.5. Schematic representation of flooding by the tsunami. Source: Analysis by IRSN of the Fukushima Daiichi Nuclear Accident of March 2011 (video), Jean-Yves Pipaud, Patrick Barra, Epsim/IRSN Media Library.

The timeline of the technical situation of the reactor units is summarized in Figure 36.6 below. Core cooling by the design-basis emergency systems is shown in green, loss of cooling in red, freshwater injection in pale blue, and sea water injection in dark blue. V stands for venting and H_2 for hydrogen explosion.

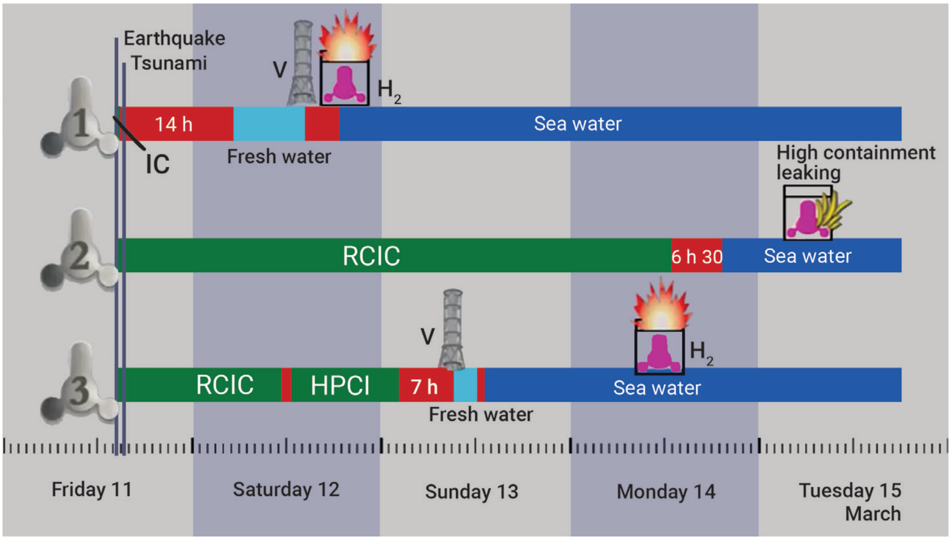


Figure 36.6. Timeline of the situation of units 1, 2 and 3. Source: Analysis by IRSN of the Fukushima Daiichi Nuclear Accident of March 2011 (video), Jean-Yves Pipaud, Patrick Barra, Epsim/IRSN Media Library.

▶ Unit 1

Following the earthquake, the isolation condenser (IC) started up automatically on a signal indicating high pressure in the reactor coolant system. To maintain the pressure between 60 and 70 bars and comply with the maximum cooling gradient permitted by the operating procedures, the operators controlled the IC manually by opening and closing the valves. After the tsunami, however, the operators no longer had information on the positions of the IC valves. Furthermore, the behaviour of these valves in the case of loss of electrical power is complex, and the operators had only limited experience in their operation: in the end the IC was no longer in service after the tsunami, but nobody was aware of this.

When indicator lamp lighting was restored at about 18:00, probably because a battery had dried, it indicated that some IC valves were closed, preventing IC operation. The operators opened the valves at 18:18, then closed them again at 18:25 in case there was a leak from an IC pipe. At 21:19, water level measurement in Unit 1 was restored using batteries removed from vehicles and connected to the back of the control panel; it indicated that the free water level was 200 mm above the tops of the fuel assemblies. This measurement, made when the reactor core was severely damaged, was in fact wrong, as shown by the curve recalculated after the accident, but the indicated value was not called into question.

At the end of the day, a shift crew member obtained a dosimeter reading of 800 μSv in ten seconds in front of the reactor building door, and a pressure sensor in the drywell, connected to a small electrical generator, indicated a value of 6 bars, well above the design pressure of the containment. These observations highlight the mistaken assessment of the situation of Unit 1.

Until then, more than eight hours after the tsunami, the members of the emergency response team were most worried about Unit 2, as they assumed that its cooling systems had failed while, lacking information, they mistakenly thought that the Unit 1 isolation condenser was operating. The day of 11 March came to a close and the core of Unit 1 was still not being cooled; it had in any case melted several hours previously.

Even so, from 17:00 on 11 March, a discussion was initiated on the use of firefighting water supplies, as the water level in the reactor vessel was still unknown and there were questions all the same about whether the IC of Unit 1 was operating properly. Deployment of such resources takes time, however, and in any case the reactor coolant system had to be depressurized before water could be injected into it. Finally, on the morning of 12 March, the operators observed that the pressure of Unit 1 had fallen, although the reason was not clearly identified. Depressurization made it possible to begin injecting fresh water, using a fire truck to pump water from reservoirs available on the site. By 14:53 on 12 March, the available fresh water resources were depleted. It was then decided to inject sea water from a pit flooded by the tsunami. About half an hour later, when the line of pipes needed was nearly ready, an explosion, doubtless due to hydrogen, blew up the upper structure of the reactor building. The explosion damaged the pipeline, which had to be repaired. Seawater injection began at 19:04. At 20:45, boric acid was added to the sea water to rule out the risk of criticality.

As stated above, the pressure in the drywell exceeded its design pressure. A containment venting command was sent at 00:06 on 12 March, 16 min after the information was obtained. However, many difficulties were encountered, including the lack of electricity, making it necessary to use temporary means, which required searching for technical documents and obtaining access to the necessary rooms and other spaces, so venting did not take place until about 14:30. During the time that elapsed until venting was implemented, leaks could have occurred at the containment head because of the observed pressure, which would explain the presence of hydrogen in the reactor building and the explosion that occurred at 15:36, mentioned above.

Core cooling was not the only concern of the emergency response team. The team had also observed, when the first pressure measurement was made since the loss of electrical power supplies, that the pressure in the drywell had exceeded its design pressure. The containment had to be preserved, and a containment venting command was sent at 00:06, 16 min after the observation, as stated above.

▶ Unit 2

After the earthquake, the shift crew started up the RCIC at Unit 2 manually, as required by procedures. The water level then rose in the reactor vessel, causing automatic shutdown of the RCIC immediately after its startup. Nine minutes later, the shift crew restarted it manually. The RCIC underwent several of these startup and shutdown cycles until the tsunami arrived on the site, and then operated for about three days, drawing water from the condensate storage tank until it was empty, then from the wetwell. However, lacking information, the operators at first doubted that it was operating properly, before they were able to confirm it visually on 12 March. Priority was thus first given to managing the situation at Unit 2.

From 12:00 on 13 March there was no more fresh water available and the order was given to prepare sea water injection in case the RCIC stopped. On the afternoon of March 13, the injection line was ready and batteries were available to power the opening of the relief valves in order to depressurize the reactor coolant system. However, it then appeared necessary to refill the pit used for this injection, already used to supply units 1 and 3. Refilling was finally not available until the morning of 14 March. At 11:01, an explosion occurred in the Unit 3 building, resulting in rubble and debris falling into the pit; the fire-fighting pumps and pipes were damaged. The RCIC failed at about 13:25 and it had not yet been possible to repair the injection line. As the HPCI was also unavailable, the core was no longer being cooled. Although the injection line was repaired in the afternoon, the reactor coolant system depressurization valves were not opened (a prerequisite) until 19:03. Meanwhile, a fire-fighting pump ran out of petrol. Sea water injection did not actually start until about 20:00. Consequently, the reactor was not cooled for about 6.5 h while, on 14 March between 16:30 and 17:30, the water level had fallen to the top of the fuel and about two hours later the fuel had melted.

▶ Unit 3

After the earthquake, the Unit 3 shift crew started up the RCIC manually, as the crew had done for Unit 2. At 11:36 on 12 March, the Unit 3 RCIC shut down. The shift crew attempted to restart it locally on the first basement level of the reactor building. They did not succeed.

However, the Unit 3 HPCI remained available and started up automatically at 12:35 on a reactor core low water level signal. The shift crew subsequently controlled the HPCI using this water level as a reference, monitoring the steam flow rate of its turbine. However, at 20:36, the water level information was no longer available because the charge of the battery supplying direct current power to the measuring instrument was too low. The shift crew then thought that water injection by the fire-fighting pumps would be more stable. At 02:42 on 13 March, it decided to shut down the HPCI manually. However, water injection into the reactor by the fire pump turned out to be impossible, as the pump discharge pressure was lower than the pressure in the reactor vessel, and the relief valves could not be opened because of the loss of electrical power supplies. The core of Unit 3 was consequently no longer cooled.

The emergency response team requested that water injection by fire trucks be prepared and that batteries be found to open the reactor coolant system relief valves. The RCS relief valves were not opened until 09:08 on 13 March. The pressure in the reactor core at last fell to a value below the injection pump discharge pressure. Sea water injection was able to start at 09:25. The core of Unit 3 was not cooled for about seven hours (from 02:42 to 09:25).

Venting the Unit 3 containment became one of the concerns of the emergency response team relatively early in the accident. The order to prepare a venting line for Unit 3 was therefore given at 17:30 on 12 March, at the same time as for Unit 2, in the hope that venting could proceed at irradiation levels that were still relatively low. The operators nevertheless encountered the same difficulties as for the other reactor units in opening the valves and keeping them open. At 08:41 on 13 March, the operators succeeded in opening the venting line, intending to keep it open during the following days to stabilize pressure in the containment, but inadvertent closures occurred. At 11:01 on 14 March, an explosion occurred in the reactor building, significantly affecting its structure.

▶ Pools

The total loss of electrical power supplies and loss of the heat sink also affected the spent fuel pools, leading to an increase in their water temperature due to decay heat from the stored fuel. The rate of temperature increase depended on the number and age of the stored fuel rods; the highest rate was in the Unit 4 pool, which contained the equivalent of three cores, including one recently unloaded from the reactor unit, releasing an estimated 2.3 MW of decay heat.

It would be several days before uncovery of the fuel assemblies would begin in the storage racks, as long as the integrity of the pools and the connected pipes was maintained. In addition, some pool water makeup had been possible, first for the pool of Unit 3 by dropping sea water by helicopter – as a reminder, the pools were in the upper part of the reactor buildings and the superstructure of Unit 3 had been destroyed by an explosion – then for the pools at units 3 and 4 by spraying fresh water from tanker trucks.

The most difficult point was undoubtedly assessing the impact of the explosions on the spent fuel pools, with potential significant loss of pool integrity and fuel uncovery, which would have strongly aggravated the situation.

In particular, at about 06:00 on 15 March, the Unit 4 building was affected by an explosion due to gases coming from the Unit 3 building through a common ventilation pipe.

Despite the explosions and loss of cooling, the fuel stored in the pools did not suffer extensive damage, but significant amounts of rubble and debris, including some very large pieces, fell into the pools of units 1, 3 and 4.

There is also a central pool located on the Fukushima Daiichi site. It was used to store the fuel assemblies from the different reactor units when their decay heat had dropped sufficiently. Therefore, despite the 6375 assemblies that it contained, the decay heat released in this pool was about 1 MW. When the tsunami struck, the pool cooling systems were also lost and its basement levels were flooded, but this central pool did not suffer significant damage during the accident.

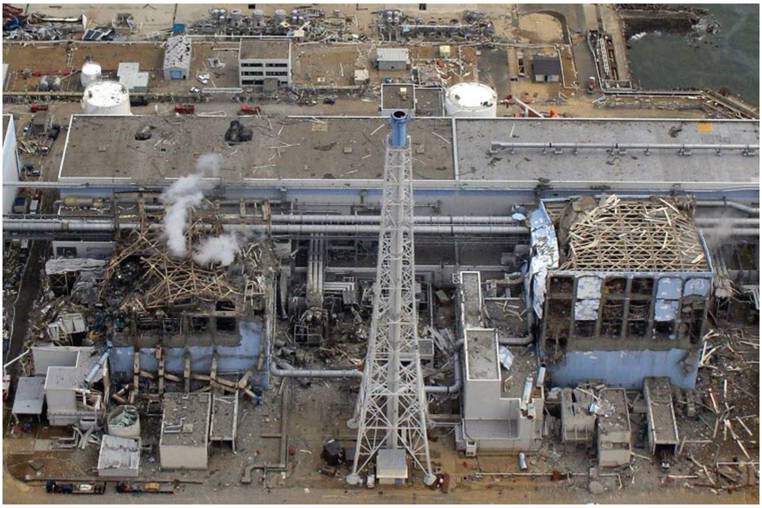


Figure 36.7. Photograph showing the destroyed superstructures of Fukushima Daiichi nuclear power plant units after the explosions. HO/AIR PHOTO SERVICE/AFP.

36.3. Radioactive release[947]

36.3.1. Airborne radioactive release, residual caesium deposits and contamination of foodstuffs

36.3.1.1. Airborne radioactive release

There were about fifteen discontinuous release episodes[948] during the 12 to 13 days following the Fukushima Daiichi nuclear power plant accident, related in particular to the agreed degassing operations.

The main radionuclides released were noble gases and short-lived radionuclides (mainly iodine-131), as well as caesium isotopes, in particular caesium-134 and caesium-137, with longer half-lives (2 years and 30 years, respectively).

The estimated activity of noble gas release was several thousand PBq (10^{15} Bq). Estimates of the total iodine-131 activity released into the air ranged from 90 PBq to 500 PBq. Estimates of activity from caesium release range from 10 PBq to 80 PBq, with equal contributions by caesium-134 and caesium-137.

In the case of the Chernobyl nuclear power plant accident, the reactor exploded, so fuel was dispersed, and plutonium and strontium-90 were found in significant quantities in the environment. In contrast, in the case of the Fukushima Daiichi nuclear power plant accident, no traces of these radionuclides were detected in the environment.

Given the atmospheric dispersion, fallout from the Fukushima Daiichi nuclear power plant accident was mainly over the Pacific Ocean, and relatively little on land, involving only a few areas of the Fukushima prefecture.

36.3.1.2. Persistent caesium deposits

Radioactive deposition following the Fukushima Daiichi nuclear power plant accident, in particular iodine-131, caesium-134 and caesium-137, was determined by the local weather. The largest deposits, along a north-west path extending for 80 km, were mainly formed in the night of 15-16 March 2011, when the wind was blowing the masses of contaminated air over the land to the north-west of the plant and a rain front was moving in the opposite direction.

[947] For further details, refer to the article in *Techniques de l'ingénieur*, *L'accident de la centrale nucléaire japonaise de Fukushima Daiichi* (The Accident at the Fukushima Daiichi Nuclear Power Plant in Japan), by E. Wattelle and P. Renaud, BN3837 V1, July 2019.

[948] During the Chernobyl nuclear power plant accident, radioactive substances were released continuously for about ten days (see Section 34.5).

Caesium-137 activity[949] on the ground reached up to three million becquerels per square metre[950].

Regarding the spread of contamination, residual caesium deposits were recorded up to 250 km away from the Fukushima Daiichi power plant.

As in the case of the Chernobyl nuclear power plant accident, radioactive substances were deposited in a 'leopard spot' pattern (see Figure 36.8). The activity deposited per unit area is more or less proportional to the precipitation (mainly rain) that occurred during passage of the radioactive plume.

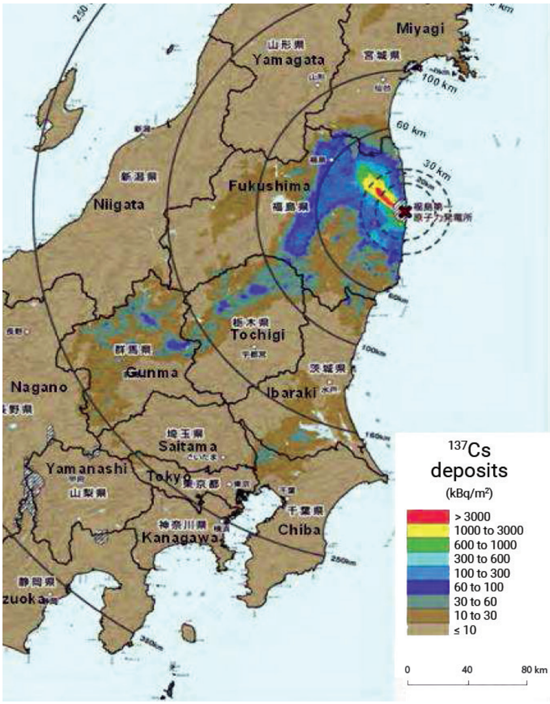


Figure 36.8. Map of persistent caesium-137 deposits resulting from the Fukushima Daiichi nuclear power plant accident (source MEXT).

36.3.1.3. Contamination of foodstuffs

Several identical observations on the contamination of foodstuffs were made after the two accidents at the Chernobyl and Fukushima Daiichi nuclear power plants:

[949] It should be noted that, in the case of the Fukushima Daiichi nuclear power plant accident, the ratio of caesium-134 and caesium-137 activities deposited was close to 1.

[950] In the case of the Chernobyl nuclear power plant accident, surface contamination reaching 20 million becquerels per m² was recorded in the most highly contaminated zones.

- the foodstuffs the most sensitive to radioactive fallout were leafy vegetables, milk (from cows grazing on contaminated grass) and, consequently, meat;
- the highest contamination levels in leafy vegetables and milk were observed immediately after deposition and decreased rapidly over the following weeks.

The activity per unit mass of iodine-131 and of caesium isotopes was very high (several tens of MBq per kilogram of fresh produce in mid-March) in grass and leafy vegetables produced in the Kawamata and Iitate municipalities before their evacuation in May and June 2011, but decreased steeply by a factor of 100 to 1000 in three months for the caesium isotopes and in one month for iodine-131.

For example, it took less than one month for contamination by radioactive iodine isotopes of spinach grown in the Fukushima prefecture to fall below the marketing limit, which was 2000 Bq/kg. This observation is explained by two factors: decay of the iodine isotopes (the radioactive half-life of iodine-131 is eight days), and natural growth of the plants, their increasing mass 'diluting' the radioactivity.

There are major differences between the two accidents at Chernobyl and Fukushima Daiichi with regard to their consequences on the contamination of field crops. The Chernobyl nuclear power plant accident occurred in the spring, when vegetation was already well developed; the plants occupied large areas and consequently 'trapped' the radionuclides considerably, leading to heavy contamination of foodstuffs. Moreover, livestock was turned out to pasture outside the barns, and so ingested the deposited radionuclides.

The Fukushima Daiichi nuclear power plant accident occurred in winter (March), when vegetation showed little growth. The proportion of radioactive deposition intercepted by plant foliage and the radionuclides transferred to the consumed parts (fruit, seeds, roots, etc.) were both low. Moreover, husbandry practices (cows housed inside buildings, fed with forage usually imported from abroad) contributed to limiting the contamination of foodstuffs.

The Japanese authorities had (and continue to have) a very large number of analyses carried out in all the monitored zones (several hundred thousand per year, including foodstuffs originating from natural sources or from the food processing industry); the analysis results are published by the Japanese Ministry of Health. For reasons discussed previously, the vast majority of foodstuffs produced in 2011 by farming or livestock-raising in Japan, including in the Fukushima prefecture, had iodine and caesium activities per unit mass below the maximum permissible levels (MPL)[951], and these activities have continued to decrease over the subsequent years.

Up to April 2012, Japanese authorities applied the maximum permissible levels (MPL) defined in Euratom regulations No. 3954/87, No. 2218/89 and No. 944/89, which aim to ensure that the dose by ingestion of foodstuffs does not exceed 1 mSv/year. The underlying assumption of the defined values is that only 10% of the foodstuffs

[951] These levels are limits for the marketing of foodstuffs, set by the Japanese government.

consumed by a person come from contaminated zones. Given that the inhabitants of contaminated regions might in fact consume 50% of foodstuffs of local origin, from April 2012 the Japanese authorities set stricter limits for caesium radionuclides; for example, the maximum permissible level for marketing leafy vegetables was reduced from 1250 Bq/kg (fresh) to 100 Bq/kg (fresh).

It is interesting to note that, as after the Chernobyl nuclear power plant accident, the activity per unit mass in forest products (game, berries, mushrooms and wild plants) decreased very little over the years; in 2019, it often still exceeded the Japanese MPL for caesium (100 Bq/kg fresh).

36.3.2. Release of radioactive substances in the Pacific Ocean

The Fukushima Daiichi power plant is located on the west coast of the Pacific Ocean, near a zone where two currents interact (Figure 36.9), leading to variable gyratory effects. These effects determine the medium- and long-term dispersion of radioactive contamination.

Run-off from the large quantities of sea water, followed by fresh water, injected into the reactors to cool them was the source of most of the contamination in the marine environment. Although most of the atmospheric release was deposited in the Pacific Ocean, the surface area in question and dilution in enormous volumes of water meant that it only made a small contribution to the radionuclide activities per unit volume observed near the coast. Nevertheless, as early as May 2011 the caesium-137 activity per unit volume in sea water within 2 km of the site had been reduced by the sea currents from several tens of thousands of Bq/L to less than 100 Bq/L. At 30 km from the plant, the caesium-137 activity per unit volume had decreased from 1000 Bq/L to about 10 Bq/L.

Subsequently, from mid-2012, measurements taken of caesium-137 activity per unit volume in sea water at distances up to 30 km from the site showed relative stability, attributed to residual release from the site, contaminated water resulting from draining of the soil in the watershed, and desorption of caesium from sediments.

At the end of 2018, caesium-137 activity per unit volume in sea water more than 30 km from the plant did not exceed 0.01 Bq/L, with even some values similar to those measured before the accident (0.001 to 0.002 Bq/L).

Contamination of water and sediments led to contamination of marine organisms. However, off the north-eastern coast of Japan, the activity per unit mass of caesium-134 and -137 no longer exceeded 100 Bq/kg (fresh) (MPL for marketing) from January 2016 for sea-bed species and from the end of 2012 for other species.

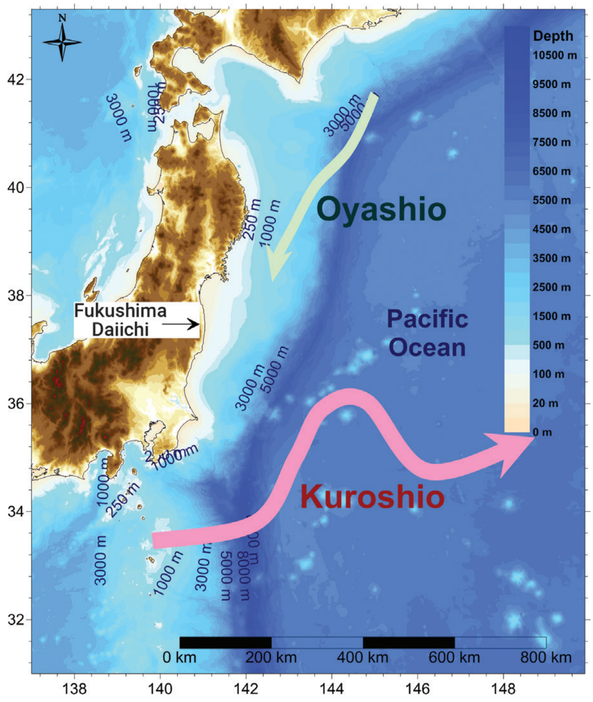


Figure 36.9. The two sea currents off the east coast of Japan near the Fukushima Daiichi power plant. Pascal Bailly-du-Bois, IRSN (source Japan Oceanographic Data Center).

36.3.3. Long-distance atmospheric dispersion of the radioactive plume

Based on the estimated releases and using the observations and forecasts provided by Météo France, IRSN modelled the atmospheric dispersion of radioactive substances released from the Fukushima Daiichi nuclear power plant over very long distances (see Figure 36.10). This model was used to define the worldwide airborne dispersion of substances released from 12 March to 1 April 2011[952]. The results were expressed in Bq/m^3 of air.

The model covered only the northern terrestrial hemisphere. The plume moved from west to east, reaching:

[952] IRSN, *L'accident de la centrale nucléaire de Fukushima Daiichi*: modélisation de la dispersion des rejets radioactifs dans l'atmosphère à l'échelle mondiale (Fukushima Daiichi Nuclear Power Plant Accident: Modelling the Worldwide Atmospheric Dispersion of Released Radioactive Substances) (2011) – Internet link: http://www.irsn.fr/FR/popup/Pages/irsn-meteo-france_30mars.aspx – Last updated on 30 March 2011.

- the west coast of the USA on 16 March, then the east coast from 18 to 19 March;
- from 22 March, Great Britain, then the Scandinavian countries;
- from 24 March, France, where iodine-131 was detected at activity per unit volume varying from a few tenths of mBq/m^3 to a few mBq/m^3; caesium-137, caesium-134 and tellurium-132 were also detected, but with activity per unit volume of a few hundredths of mBq/m^3.

In April 2011, IRSN estimated that the activity per unit volume in rainwater in France was a few Bq per litre. Precipitation of 100 mm in one month could therefore result in radioactive deposits of a few hundred Bq per m^2, much lower than the values that resulted from the Chernobyl nuclear power plant accident (up to a few thousand or even tens of thousands of Bq per m^2 in eastern France). In France, from 30 March to 10 April 2011, i.e. during and after the passage of the Fukushima Daiichi plume, very low levels of iodine-131 and caesium-134 were detected in grass (from 0.5 to about 10 Bq/kg fresh product) and the soil.

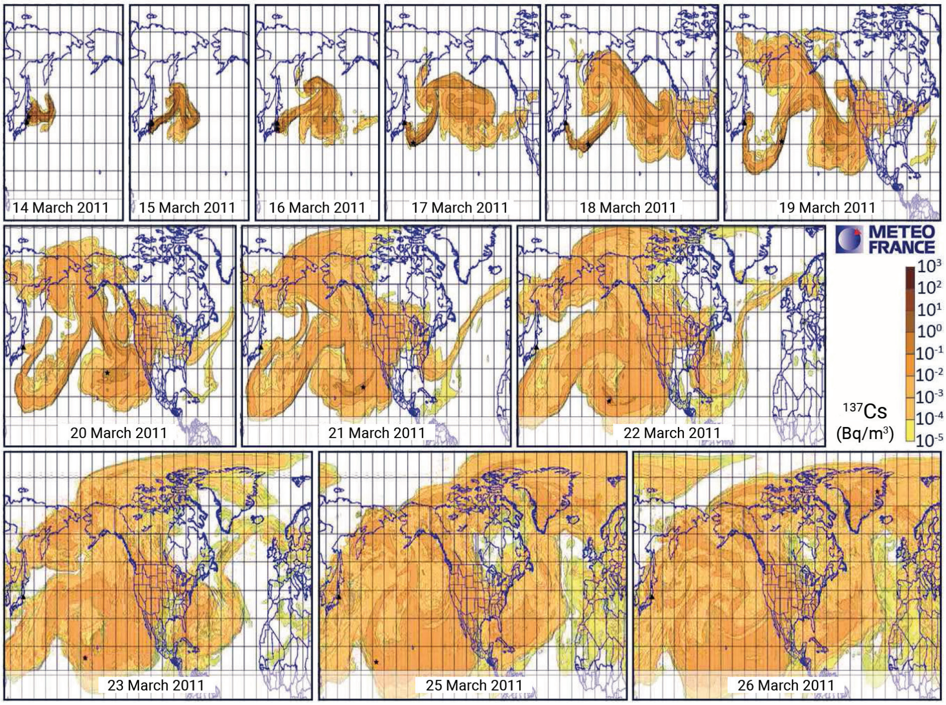


Figure 36.10. Météo France – IRSN calculated dispersion of the radioactive plume from the Fukushima Daiichi nuclear power plant (caesium-137). Météo France – source IRSN.

36.4. Action taken to control facilities and released contaminated water

Some of the most significant post-accident actions are described below (based on the situation at the end of 2019)[953].

Following the events described above, most of the facilities on the Fukushima Daiichi nuclear power plant site were devastated: the tsunami had not only flooded the buildings, but also deposited large amounts of debris on the site; units 1, 3 and 4 had suffered large explosions, damaging their structures, and the cores of units 1 to 3 had melted. It was necessary to gradually restore long-term control of the facilities and the radioactive substances that were still likely to be released from them, given their damaged state, especially the containments, and the large amounts of contaminated water produced since the accident. Managing contaminated water turned out to be particularly complicated.

▶ Functional control of the facilities

The cores of units 1 to 3 must still be cooled, even though the decay heat that they generate has decreased significantly, allowing much more time to respond to any cooling failures than what was possible during the accident. Cooling is provided by injecting fresh water (at a flow rate below 5 m^3/h per reactor and at a temperature generally below 30°C) into the vessels of units 1 to 3. Because the vessels and containments are not leaktight, the injected water flows into the building basements, where it mixes with infiltrated groundwater. The water is pumped from the basements, treated, then reinjected into the reactors. The spent fuel pools are cooled by closed-loop cooling, with pumps circulating water continuously through a loop equipped with a heat exchanger. The heat exchanger is in turn cooled by another closed loop, itself cooled by an air-cooled exchanger. The temperature in these pools is also generally lower than 30°C.

Nitrogen was injected as needed into the containment and vessel of units 1 to 3 in order to keep the atmosphere inert, thereby avoiding any risk of hydrogen combustion.

The means implemented are redundant and emergency power supplies are provided; some equipment has been installed in elevated areas.

▶ Control of released substances

To reduce release to the atmosphere, the facility operator, TEPCO, has made a particular effort to restore confinement of the reactor buildings. By October 2011, it had already covered the building of Unit 1 with a structure. This structure was gradu-

[953] IRSN has published on its website a document entitled *Suites de l'accident nucléaire de Fukushima Daiichi en mars 2011 – Point de la situation en mars 2016* (Follow-up on the Fukushima Daiichi Nuclear Power Plant Accident in March 2011 – March 2016 Update), which provides more details on the topics discussed in sections 36.4 and 36.5.

ally dismantled from 2014 to 2017, but just enough so that debris could be removed from the building; it will eventually be replaced by a new structure. A new, complete structure was installed on the Unit 4 building between January and July 2013: in addition to control of released substances, it was also designed so that fuel assemblies could be removed from the pool. Similar work was also carried out on the Unit 3 building from August 2017 to February 2018. Roofing on the Unit 2 building had not been damaged. The only roof work carried out was reinforcement of an opening. However, a new structure is also to be installed in preparation for fuel removal operations; the removal of the fuel assemblies from the pools in units 1 and 2 was planned for some time in 2020. Agents used to limit dust dispersion have been sprayed on the buildings. Spraying is also generally carried out before work on the buildings.

It is also necessary to limit infiltration of groundwater (which circulates naturally from inland towards the ocean) into the building basements, where it is contaminated by mixing with the water used to cool the reactors, so that it has to be treated and stored.

Treatment capacity has now been sized to handle considerable volumes: all the stored water has been treated[954] to remove caesium and strontium; most of the water has also undergone more complete treatment and contains only tritium[955], along with traces of other radionuclides. However, discharge of the treated water that has passed through the Fukushima Daiichi nuclear power plant buildings is not permitted by Japanese authorities. Consequently, the volumes stored in tanks on the site are increasing inexorably, now exceeding 1,000,000 m^3.

Various systems have been installed to control groundwater flows (see Figure 36.11), in particular:

- a groundwater bypass pumping system upstream of the buildings, set into service from April 2014: the pumped water is discharged after testing;
- water drainage on the periphery of the buildings (subdrains), by repairing 27 existing relief wells and building 15 new wells, to lower the groundwater level;
- a system for freezing the ground (forming a landside impermeable wall) to a depth of some 30 m around units 1 to 4 (within a perimeter of about 1500 m): 1552 boreholes were drilled for freeze pipes between June 2014 and October 2015 to circulate a liquid at very low temperature. The entire perimeter has been frozen since 2018.

[954] TEPCO rapidly implemented various processes for radionuclide removal from contaminated water. One process is no longer used, as it produced a large volume of radioactive sludge. TEPCO then initiated the development of a system for more complete treatment, the multi-nuclides removal equipment or Advanced Liquid Processing System (ALPS). This system has been in operation since October 2014.

[955] There is currently no industrial process for treating tritium, although research in this direction is underway.

The pumped water is treated and discharged after testing, in agreement with the local fishermen's associations[956] and Japanese authorities.

To keep contaminated groundwater from reaching the ocean, a leaktight barrier (a seaside impermeable wall, consisting of metal tubes) has been installed along the port; it is 35 m high (more than half of which is buried in the ground down to the water-tight stratum) and nearly 900 m long. In 2014, the space between the wall and the protection dyke was filled in and five pumping wells down to the deepest groundwater were installed and tested; this system entered into service in October 2015. The pumped water is treated and tested before discharge.

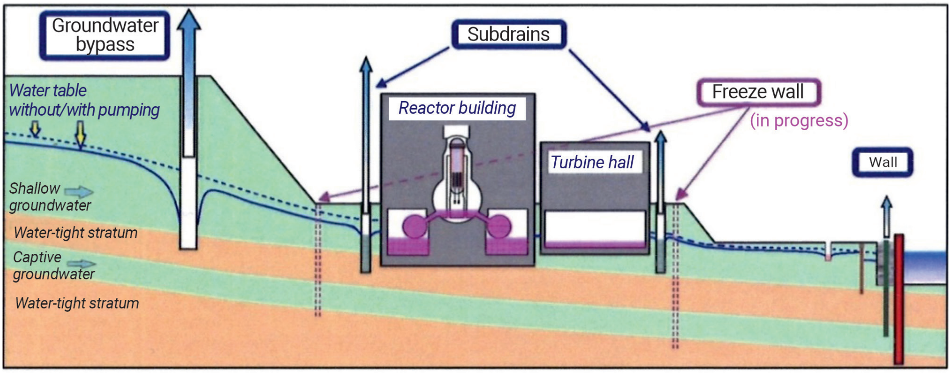


Figure 36.11. Diagram showing the bypass and subdrain systems for groundwater drainage, the freeze pipes around the reactor buildings, the seaside wall and the associated pumping pipes. TEPCO.

▶ Facility dismantling

The facilities will eventually be completely dismantled. The mid- and long-term roadmap has been divided into three phases:

- removal of fuel assemblies from the reactor cavities. Removal of fuel assemblies from the Unit 4 cavity, containing the largest number of assemblies, was completed in December 2014. Removal of the major debris from the upper floor of the Unit 3 cavity, construction of a structure sheltering the handling systems needed for unloading the assemblies, and installation of these systems have been completed; fuel assembly removal began in April 2019. Removal of the fuel assemblies from the cavities of units 1 and 2 is scheduled for 2023;

[956] For discharges, TEPCO, in agreement with fishermen's associations and authorities, sets contamination limit values below the discharge values given in Japanese regulations: less than 1 Bq/L of caesium-137, less than 1500 Bq/L of tritium, and less than 3 Bq/L or 5 Bq/L of total beta emission (mainly strontium) depending on the water catchment system.

- removal of damaged fuel from units 1 to 3. This phase is obviously more complicated, and its completion depends on a major research programme undertaken for this purpose. Means of investigation must be developed to complement those deployed until now for the sole purpose of obtaining more detailed knowledge of the state of the facilities. Specific investigations and inspections are gradually being conducted in the facilities, including by sending robots into the containments. The means required to remove the reactor cores will then have to be defined and designed. Damaged fuel is scheduled to be removed before 2025;
- complete dismantling of the facilities; the time required cannot yet be given, but the objective is 30-40 years.

36.5. Socioeconomic and health impact in numbers

36.5.1. Socioeconomic impact

Early in April 2011, the harsh socioeconomic impact[957] of the Fukushima Daiichi nuclear power plant accident was felt by the population. The residents of the exclusion zone, with a radius of approximately 20 km around the plant, were evacuated, and the residents of the zone between 20 km and 30 km from the plant were instructed to stay at home or evacuate voluntarily by their own means. Environmental contamination required a ban on the sale of milk and various agricultural products in several prefectures (in particular north-west of the plant); sales of marine products were also banned, with fishing suspended within a radius of 30 km around the site, reduced to 20 km at the end of September 2011. Japanese wholesalers and consumers avoided all foodstuffs from these regions, depriving farmers of income. The inhabitants of the most severely affected municipalities (in particular Iitate[958]) spent several weeks waiting for aid from the government or a possible evacuation order. Their evacuation was finally ordered late on 11 April.

The socioeconomic consequences affected not only the Special Decontamination Areas but also the more extensive Intensive Contamination Survey Areas (zoning established by public authorities, as explained in Section 36.5.2).

The combination of earthquake, tsunami and nuclear accident had a direct effect on the Japanese economy. Exports fell by 2.4% in April 2011 compared with the level in April 2010. At the same time, imports increased, especially those related to fuel, chemicals and food, resulting in a deficit in the trade balance in April and May 2011. Fossil fuel imports subsequently remained at a high level.

The considerable reduction in nuclear generation of electricity (about -94% between 2010 and 2016) was compensated by increased electricity generation by

[957] The sources used include the article Energy in Japan (Wikipedia), and the *Connaissance des énergies* (Energy Knowledge Base) website.

[958] The village of Iitate is located 39 km north-west of the Fukushima Daiichi nuclear power plant.

sources such as coal, natural gas and solar power; over the same period a decrease in consumption was observed (-6%), due in part to a 25% increase in the price of electricity between 2011 and 2014. The Basic Energy Plan approved on 3 July 2018 by the cabinet of Japan's Prime Minister for 2030 calls for a power generation mix of 20% to 22% nuclear energy, 22% to 24% renewable energies and 56% fossil energies. Five out of 54 nuclear power reactors remained in service after the Fukushima Daiichi nuclear power plant accident. When the new safety standards approved in Japan after the Fukushima Daiichi nuclear power plant accident were taken into account, only 39 of the Japanese nuclear power reactors were considered as fit for operation. As of the end of 2018, 11 reactors operated by various electricity utility companies (Kyushu Electric Power, Shikoku Electric Power, Kansai Electric Power, TEPCO) had been restarted with the approval of the new Japanese nuclear safety authority (NRA, see Chapter 37). For example, in 2017 TEPCO obtained NRA approval for restarting two of the boiling water reactors, upgraded to the new safety standards, of the Kachiwazaki-Kariwa nuclear power plant (which has seven BWRs) – this plant had suffered a major earthquake in 2007. In addition, three reactors are under construction.

Revitalization initiatives and reconstruction activities undertaken within the framework of a 'recovery'[959] process range from those conducted by public authorities at national level to initiatives by non-governmental organizations and local communities. The Japanese government has established a Reconstruction Agency, the Fukushima prefecture has taken various initiatives, including the founding of the Centre for Environmental Creation, while TEPCO established the Fukushima Revitalization Headquarters in 2013. All these projects aim to reconcile radiation protection measures with broader societal aspects, such as revitalization of infrastructure, engagement and – in the case of the Revitalisation Headquarters – compensation of the population. An example of a successful revitalization initiative is the cooperation established between producers and distributors of peaches, on one hand, and the food processing industry, on the other hand, to restore public confidence in the foodstuffs produced in the Fukushima prefecture.

36.5.2. Health impact

Over the period following the Fukushima Daiichi nuclear power plant accident, from 11 March to October 2011, Japanese authorities recorded seven deaths among the 25,000[960] people who worked on the plant site; overall, five of these deaths were attributed to the accident (two by drowning in the tsunami, three by heart attack), but

[959] Post-accident recovery includes: the remediation of areas affected by the accident; the stabilization of damaged on-site facilities and preparation for decommissioning; the management of contaminated materials and radioactive waste arising from these activities; community revitalization and stakeholder engagement. Remediation is defined as any measures that may be carried out to reduce radiation exposure from existing contamination of land areas through actions applied to the contamination itself (the source) or to the exposure pathways to humans.

[960] Of these 25,000 workers, about 3600 were TEPCO employees and almost 22,000 were employees of subcontractors.

no deaths were attributed to exposure to ionizing radiation. An estimated further 40 to 50 deaths were a consequence of the evacuation of the contaminated territories, among the 20,000 to 50,000 persons evacuated.

Assisted by a large number of specialists[961], international organizations have produced and published reports on the health impact of the accident, in particular:

- the World Health Organization – WHO; in 2012-2013 the WHO published reports providing a preliminary evaluation of the doses received by the persons exposed as a consequence of the Fukushima Daiichi nuclear power plant accident, and an analysis of the resulting health risks;
- the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR), which in 2014 published a report (dated 2013) including an estimation of the levels and effects of radiation exposure attributed to the accident, based on a large body of data on radioactivity in the environment at Fukushima and irradiation doses received.

The discussion in the rest of this section is based on these reports[962].

In the short term, the most significant contributors to public exposure were:

- external exposure from radioactive substances released to the atmosphere and radionuclides deposited on the ground,
- internal exposure of the thyroid gland due to intake of iodine-131 and internal exposure of other organs and tissues, mainly due to intake of caesium-134 and caesium-137.

In the long term, the most important contributor to public exposure is external radiation from caesium-137 deposits.

With regard to occupational exposure, after the accident, the members of the on-site emergency response teams worked in extremely difficult conditions, and the radiation levels were very high while they worked to stabilize the state of the reactors. From March 2011 to March 2012, 174 emergency workers on the Fukushima Daiichi nuclear power plant site received an effective dose exceeding the initial 100 mSv limit for emergency situations, and six emergency workers also exceeded the temporarily revised effective dose limit of 250 mSv. No workers received an effective dose of 100 mSv during the subsequent years.

The main internal doses were thyroid equivalent doses due to iodine-131 intake. Although most of the emergency workers at the Fukushima Daiichi nuclear power plant received thyroid equivalent doses below 100 mSv, 1757 of them received higher

[961] Nine French specialists took part in work conducted by UNSCEAR (five from IRSN and four from CEA).

[962] As well as the IAEA report entitled The Fukushima Daiichi Accident published in 2015. This book is based on information available at the time it was finalized.

doses, including 17 who received doses greater than 2000 mSv and 2 who received doses greater than 12,000 mSv[963].

Although no early radiation-induced health effects that could be attributed to the accident were observed among workers or members of the public, the possibility of delayed health effects must be taken into account, as the latency time before the appearance of late radiation health effects can be decades. However, according to the UNSCEAR report, "no discernible increased incidence of radiation-related health effects are expected among exposed members of the public and their descendants". UNSCEAR concluded that, among the group of workers who received effective doses of 100 mSv or more, "an increased risk of cancer could be expected in the future. However, any increased incidence of cancer in this group is expected to be indiscernible because of the difficulty of confirming such a small incidence against the normal statistical fluctuations in cancer incidence."

A Fukushima health management survey was conducted to monitor the health of the affected population in the Fukushima prefecture. This survey aimed to ensure early detection and treatment of diseases, as well as the prevention of lifestyle-related diseases. Intensive screening of the thyroid gland in children was implemented as part of the survey.

Lastly, the UNSCEAR report provides information on the psychological consequences of the Fukushima Daiichi nuclear power plant accident. UNSCEAR estimated (in 2013) that "the most important health effect is on mental and social well-being, related to the enormous impact of the earthquake, tsunami and nuclear accident, and the fear and stigma related to the perceived risk of exposure to ionizing radiation. Effects such as depression and post-traumatic stress symptoms have already been reported."

▶ Off-site remediation of areas affected by the accident

A remediation policy was enacted by the Japanese government in August 2011. It assigned responsibilities to national and local authorities, and to the facility operator. The policy focuses on decontamination activities to reduce the levels of radioactivity due to radiocaesium deposited on the ground in priority areas (residential areas, including buildings and gardens, farmland, roads and infrastructure), with the aim of reducing external exposure of the population. Internal doses continue to be controlled by restrictions on food, as well as through remediation activities on farm land. A distinction was made between two categories of contaminated areas based on additional annual doses estimated in the autumn of 2011. The national government was assigned responsibility for formulating and implementing remediation plans in the first area (the 'Special Decontamination Area') within a radius of 20 km from the Fukushima Daiichi site and in areas where additional annual doses arising from soil contamination were projected to exceed 20 mSv in the first year after the accident.

[963] TEPCO, Evaluation of the Exposure Dose of Workers at the Fukushima Daiichi Nuclear Power Station. Attachment: distribution of thyroid equivalent doses, 2015.

Municipalities were given responsibility for implementing remediation activities in the other area (the 'Intensive Contamination Survey Area'), where the additional annual doses were projected to exceed 1 mSv, while remaining below 20 mSv. Specific dose reduction goals were set, including a long-term goal of achieving an additional annual dose of 1 mSv or less.

36.6. Lessons learned from the accident

The accident that affected the Fukushima Daiichi nuclear power plant reactors was a major shock. Japan gradually shut down all of its nuclear power reactors: those that were already shut down when the earthquake occurred or shut down as a consequence of it remained shut down; in May 2011 the Japanese government decided to shut down units 4 and 5 of the Hamaoka nuclear power plant, located on Japan's east coast and operated by Chubu Electric Power, pending reinforcement of site protection; the other reactors were not authorized to restart once they had reached their scheduled maintenance outage. Only two units (Ohi 3 and 4, located in western Japan and operated by Kansai Electric Power) were able to complete an operating cycle between 2012 and 2013. Returning nuclear power reactors to service in Japan was subject to the implementation of improvements to meet the new safety standards laid down by the new nuclear regulatory authority (NRA). A large number of verifications by the NRA were required before a reactor could be authorized to resume operation, as was the case in 2015 for Unit 1 of the Sendaï nuclear power plant operated by Kyushu Electric Power on Kyushu Island, and in 2017 for two reactor units of the Kachiwazaki-Kariwa nuclear power plant operated by TEPCO (see Section 36.5.1).

Many safety lessons were learned from the Fukushima Daiichi nuclear power plant accident. Beyond the fact that the dyke was too low, which was the primary cause of the accident, underlining the importance of site selection and taking into account environmental risks, many other facts deserved more in-depth analysis.

With regard to the tsunami risk[964], the Fukushima Daiichi nuclear power plant had been designed and built with protection against flooding by a water level at +3.1 m with respect to the mean sea level[965]. The reactor platforms were built at +10 m for units 1 to 4 and at +13 m for units 5 and 6; however, some equipment important to plant safety had been installed close to the sea at +4 m, including ultimate heat sink equipment and emergency generator cooling equipment.

In 2002, TEPCO had revised the water level that could be induced by a tsunami to +5.7 m[966]. As a result, buildings were rendered leaktight and the reactor residual heat removal equipment pump motors located at +4 m were raised.

[964] IAEA report The Fukushima Daiichi Accident, report by the Director General, 2015.

[965] This value is the water level of the tsunami recorded in the port of Onahama, located 50 km south of Fukushima Daiichi, after the Chilean earthquake on 24 May 1960.

[966] Runup height (maximum wave).

In 2009, TEPCO and other Japanese facility operators had again revised the flood levels that could result from tsunamis, using a method based on a standard source model for tsunamis, developed by the Japanese Society of Civil Engineers and published in 2002; in 2009, the tsunami maximum height had been revised to +6.1 metres, leading TEPCO to further raise the pump motors of the reactor residual heat removal system.

Before the accident, TEPCO had conducted new evaluations using a method developed by the Japanese Headquarters for earthquake Research Promotion, based on another tsunami source model and using more recent data, postulating an earthquake of magnitude 8.3 off the Fukushima coast, stronger than in the previous evaluations. The new evaluation gave an amplitude of +15 m at the site, similar to the actual height recorded on 11 March 2011. On the basis of this new evaluation, TEPCO, NISA[967] and other Japanese organizations had judged that further studies and research were necessary. TEPCO and other power companies had consequently asked the Japanese Society of Civil Engineers to review the appropriateness of the tsunami source models; this work was in progress in March 2011.

In Japan, committees were mandated by the government or by the parliament and communicated their conclusions without compromise. In particular, they were highly critical of the nuclear safety authority (see Chapter 37). The problems of managing the emergency were also underlined.

The various organizations concerned, in other countries as well as in Japan, were obliged to call into question their safety approaches. The remainder of this chapter mainly covers the 'complementary safety assessments' conducted in France. Some other initiatives and actions at international level are discussed in Chapter 37.

36.6.1. Complementary safety assessments carried out in Europe and France following the Fukushima Daiichi nuclear power plant accident

On 23 March 2011, the French Prime Minister asked the president of the French nuclear safety authority, ASN, to conduct a study on the safety of nuclear facilities, giving priority to nuclear power reactors, in view of the accident that had just occurred in Japan. The study had to cover five points: the risks of flooding, earthquake, loss of power and loss of cooling, and emergency response management in accident situations. The Prime Minister requested that each facility be studied individually to determine whether improvements were necessary in light of lessons learned from the Fukushima Daiichi nuclear power plant accident, in a manner consistent with the work being done at European level by ENSREG (European Nuclear Safety Regulators Group) and WENRA (Western European Nuclear Regulators Association); he asked for the initial conclusions of the study to be submitted before the end of 2011.

[967] Nuclear and Industrial Safety Agency.

Meanwhile, the European Council, at its meeting on 24 and 25 March 2011, invited the European Commission and ENSREG to conduct a "comprehensive and transparent risk and safety assessment" of all the nuclear power plants in the European Union in light of the Fukushima Daiichi nuclear power plant accident, based on stress tests to be conducted by facility operators. The technical specification for these stress tests was defined on the basis of a proposal by WENRA. The stress tests were intended to assess the 'response' of facilities to extreme situations, mainly concerning earthquakes, flooding, loss of power, loss of ultimate heat sink, and emergency response management of severe accidents that could have long-term effects on all or part of the facilities on a site. The assessment was intended to identify any weak points in the facilities and the associated 'cliff edge' effects in order to define possible technical or organizational improvements.

In France, the study requested by the Prime Minister led to complementary safety assessments carried out by facility operators, applying a specification based on the WENRA proposal for stress tests, but extended to practically all nuclear facilities and, after consultation of the French High Committee for Transparency and Information on Nuclear Safety (HCTISN), supplemented by a section relevant to contractors working for the facility operators.

The conclusions of the stress tests conducted by facility operators in 2011 were subjected to independent review by each national nuclear regulator concerned. At European level, peer review of the conclusions of these reviews, supplemented by site visits, resulted in April 2012, one year after the accident, in the production of a report in each country, a general report by ENSREG[968], and the definition of an action plan by each country, with follow-up at European level. It should be noted that Switzerland and Ukraine, although outside the European Union, were full participants in the process. Overall, according to the conclusions of the peer review, "the stress tests identified tangible improvements". In this regard, the general report emphasizes that significant measures to improve the robustness of the nuclear power plants with regard not only to hazards, but also to situations of total loss of cooling water or of electrical power, have been decided or are under study in the various European countries, including, for example, the definition of reinforced equipment and appropriate preparation for such hazards and situations. Four recommendations were put forward in the general report concerning the need for additional guidance on assessment of natural hazards, the promotion of periodic safety reviews, implementation of measures to protect containment integrity, and reinforcement of accident prevention and mitigation.

For the most part, the report on France recommended completing deployment of the improvements proposed by EDF or requested by ASN (see below), noting in particular the approach implemented, which led to the post-Fukushima 'hardened safety core' concept, an approach described in greater detail below. Several recommendations were also made on taking into account natural phenomena (in particular

[968] Refer to http://www.ensreg.eu/EU-Stress-Tests for more detailed information on this topic.

the implementation of probabilistic approaches for characterization of low-probability unforeseen events).

The European Council meeting on 28 and 29 June 2012 and the technical summary produced by the European Commission in October 2012 confirmed the conclusions of the reports cited above.

Each country then produced an action plan at the end of 2012, which is now subject to follow-up.

36.6.2. Complementary safety assessments carried out in France

The complementary safety assessments conducted in France must be placed in the context of the continuous search for facility safety improvements, based on elements discussed in the previous chapters:

- practical application of event-based operating experience feedback,
- periodic reviews, including verification that facilities are in compliance with applicable requirements, and reassessment of facility safety in light of new knowledge, new requirements, etc.,
- development of new baselines or reassessment of existing baselines, independently of periodic reviews (for example, with regard to taking into account severe accidents or assessment of flooding risk).

Considering the events that affected the Fukushima Daiichi nuclear power plant reactor units, it should be noted that the safety baselines for French nuclear power reactors in operation already covered:

- situations involving total loss of reactor off-site and on-site power for a period of 24 h,
- situations involving total loss of the reactor heat sink for a period of 100 h.

Partial flooding of the Blayais nuclear power plant in late 1999 (see Section 24.1) had also led EDF to conduct studies on the reserves available on site for managing a total loss of off-site power or loss of heat sink, as well as a combination of these two situations. In these studies, one of the possibilities assessed was loss of off-site power due to an earthquake, which had led EDF to postulate such a loss over a period of 15 days, significantly longer than the duration used in the initial design studies, leading to modifications of the emergency generators to improve their long-term reliability. However, other improvements were still necessary, in particular an increase in the secondary water reserves.

These studies were already a notable advance in taking into account the risks of loss of power or loss of cooling for the entire plant in the event of a hazard.

36.6.3. Procedure for complementary safety assessments carried out in France

The Prime Minister's request discussed above was sent to nuclear facility operators[969] by ASN in a letter dated 5 May 2011, which translated the five points in the request into requirements – with an added section on the use of contractors – asking them in particular to describe for each facility:

- "measures taken in facility design and compliance of the facility with the applicable design requirements,
- the ability of the facility to withstand beyond-design-basis conditions, in particular by identifying situations leading to sudden degradation of the accident (cliff edge effect) and measures taken to avoid these situations,
- proposals for reinforcing facility safety and emergency response management."

The deadlines prescribed for EDF were as follows:

- communication of the method selected for conducting the complementary safety assessments: no later than 1 June 2011,
- communication of a preliminary report[970]: no later than 15 September 2011 for reactors in operation and the Flamanville 3 EPR, and no later than 15 September 2012 for reactors in the dismantling phase.

ASN asked the Advisory Committees for their opinion on the conclusions of the complementary safety assessments carried out by facility operators and the pertinence of the proposed improvements they had submitted within this framework. This opinion, sent to ASN in November 2011, was based on IRSN's assessment of the documents submitted by facility operators.

In parallel with the review of these documents, ASN conducted a wide-ranging programme of inspections on the five topics defined in the Prime Minister's letter. These inspections were conducted from 17 June to 21 October 2011 and concerned all the sites for which the complementary safety assessment report had to be submitted in 2011.

The schedule defined both at the national level for completion of the complementary safety assessments and at European level for completion of stress tests was extremely tight, given the large number of facilities concerned and the technical expertise required to answer the questions raised.

EDF submitted its reports in mid-September 2011 and IRSN issued its assessment report in early November 2011. Based on this assessment and the conclusions of the Advisory Committee opinions, ASN published its report on the complementary safety assessments of French nuclear facilities at the beginning of 2012, less than 10 months after the accident.

[969] For EDF, this was ASN decision 2011-DC-0213 of 5 May 2011.

[970] "Using available data and based on the existing safety studies and engineer's judgement."

36.6.4. Conclusions of the complementary safety assessments carried out in France

The complementary safety assessments first of all confirmed that French nuclear power reactors in power plants that complied with the applicable safety requirements were capable of withstanding the natural hazards defined for the various sites (considered at the reactor design stage or in more recent safety reassessments). Moreover, given the methods and the design criteria used, in most cases it could be estimated that the facilities would be capable of coping with natural hazards of greater severity than those considered when they were designed or in safety reassessments – even though the margins were not necessarily easy to determine.

The complementary safety assessments underlined and served as a reminder of the primary importance that must be given to keeping facilities in compliance with applicable safety requirements throughout their operating lifetime.

EDF also proposed the implementation of specific measures, based on equipment on the site or transportable to the site in the event of an accident, to enhance facility resistance to natural hazards. The proposals included:

- installing an additional generator, the ultimate diesel generator (UDG), for each nuclear power reactor in operation, to provide long-lasting backup power in the event of total loss of all other facility power supplies,
- where necessary, duplicate certain equipment items common to more than one reactor on a given site in order to manage an accident situation affecting two or more reactors simultaneously.

However, one of the most immediate measures taken by EDF was its undertaking to establish a Nuclear Rapid Response Force (FARN), tasked with assisting any French nuclear power plant in the management of a severe accident situation; the first-response units would be dispatched to the facility within 24 h.

IRSN, in its assessment report, concluded that a more complete set of measures should be implemented at the facilities to respond to situations involving a loss of power or loss of heat sink that could be caused by more severe natural hazards than considered previously, pending the arrival of FARN assistance.

The specific approach developed by IRSN in its analysis of the proposals submitted by EDF led IRSN to suggest the implementation of a ‘hardened safety core’ concept, consisting of equipment, organizational and human resources capable of maintaining, at least during the first few days following the accident, the vital safety functions of the plant systems at the facility in the event of total loss of cooling sources or electrical power, in particular following a beyond-design-basis external hazard, with FARN deployment then engaging management of the accident over the longer term.

This concept was discussed at meetings of the Advisory Committees and, for the most part, met with their approval.

Although conducted within extremely short time limits, the complementary safety assessments provided the basis for:

- assessing whether existing measures were compliant with the applicable safety requirements regarding external hazards such as earthquakes or flooding, and losses of heat sink and electrical power supplies,
- identifying the changes to be made in existing safety baselines without waiting for the next periodic reviews (determining the levels to be applied to earthquake and external flooding hazards, hazard combinations to be considered, etc.),
- defining the 'hardened safety core' concept and prescribing its implementation.

ASN decisions dated 26 June 2012 formulated additional requirements for EDF[971], including a request to submit a proposed hardened safety core design before 30 June 2012, capable of:

- "preventing a fuel-melt accident or limiting its progress,
- limiting massive release of radioactive substances,
- enabling the facility operator to fulfil the missions for which it is responsible in emergency management."

36.6.5. The 'hardened safety core'

36.6.5.1. Purpose

As discussed above, the purpose of the hardened safety core is to limit radioactive releases likely to have major short-, medium- and long-term consequences in situations of lasting loss of power or loss of heat sink at a facility, including in the case of an extreme external hazard. If no emergency system is operational rapidly, these situations lead to reactor core melt and, in the longer term, to uncovery of the fuel assemblies stored in spent fuel pools.

It is essential to reduce the radiological consequences of such accidents as far as reasonably achievable, particularly as, in the event of a natural disaster of the kind that occurred in Japan in March 2011, the facility environment would be severely damaged, making it difficult to take action to protect the population near the facility and, in the longer term, to manage the contaminated areas.

36.6.5.2. Principles

For nuclear power reactors, in accordance with the ASN decisions of 26 June 2012 mentioned above, the hardened safety core must prevent a fuel-melt accident, limit its progress, limit radioactive release and enable emergency response management.

[971] Decisions were issued for each NPP.

In a decision dated 21 January 2014, ASN also informed EDF of the situations to be taken into account in designing the hardened safety cores, and in particular the hardened safety core design-basis earthquake:

- The hardened safety core situations to be taken into account are:
    - "total loss of power supplies that are not part of the hardened safety core,
    - total loss of the [reactor cooling] heat sink that is not part of the hardened safety core,
    - the external hazards defined for the hardened safety core,
    - situations arising from the state of the facility, the site and its environment after one or more external hazards defined for the hardened safety core."
- The hardened safety core design-basis earthquake must:
    - "encompass the seismic margin earthquake (SME) for the site, augmented by 50%,
    - encompass the spectra defined using a probabilistic approach for a 20,000-year return period,
    - take into account particular site effects, especially the soil type."

The hardened safety core thus comprises measures enabling fulfilment of all the fundamental safety functions defined in Chapter 6 in the situations and conditions discussed above, also taking into account both reactors (whether the facility is operating at full power or shut down, including when the reactor building is open) and spent fuel pools.

In addition, the hardened safety core must be defined by considering the loss of all the measures already implemented in facility design, when it is not possible to demonstrate the ability of these measures to withstand natural hazards significantly more extreme than those taken into account in facility design.

It must also be possible for the facility operator to fulfil its responsibilities in emergency situations. For this purpose, the hardened safety core measures must ensure that emergency response teams can access the information needed to assess the state of the plant systems and to prepare on-site operations. If radioactive substances are released to the environment, the facility operator must also be able to assess the consequences of the release based not only on data available from the plant systems, but also on measurements taken in the environment (meteorological measurements, dose rate and activity measurements): this information must allow the facility operator and public authorities to take decisions within the scope of their respective responsibilities to protect personnel on site and the public. In this context, it is therefore vital for the facility to have operational external communication systems in the situations under consideration.

The hardened safety core must be able to deal with situations where the various levels of protection provided in the initial design of plant systems may be inadequate, since it has not been demonstrated that these systems can withstand situations more severe than those taken into account in system design. The introduction of measures that are, as far as possible, independent and diversified with respect to existing measures is then a structuring factor for obtaining a high level of confidence in the capacity of the hardened safety core to fulfil its functions.

In the definition of the hardened safety core, special attention must also be given to support systems necessary for the operation of systems that directly perform safety functions. These include electrical power generation and distribution systems (generators or batteries, electrical switchboards), instrumentation and control systems, and ventilation systems (for thermal conditioning of rooms). For these systems, the objective is to ensure that they are independent from existing systems and are diversified with respect to them.

For existing reactors, it was not possible to design a hardened safety core consisting exclusively of new equipment. The definitive hardened safety core therefore consists of existing structures, systems and components (SSCs), reinforced as necessary so that they will be operational in the event of a beyond-design-basis hazard, as well as new SSCs.

Another principle applied is that the hardened safety core must consist mainly of stationary systems for managing the on-site situation until the FARN arrives. The use of mobile equipment when the facility and its environment could be very severely degraded and available human resources could be limited may not, in practice, provide sufficient guarantees. Stationary equipment, however, must be installed in bunkers so that it can operate in the event of a beyond-design-basis hazard and can be protected against the effects induced by the hazard in the facility (falling loads, fire, explosion, etc.). The extreme hazards taken into account for the definition of the hardened safety core are earthquake, flooding, and extreme weather conditions, including tornadoes.

36.6.5.3. Illustrations

▶ Reactors

The new measures taken by EDF in the hardened safety core to fulfil the fundamental safety functions are explained below (Figure 36.12):

- the chain reaction will be stopped automatically by inserting RCCAs in the core upon detection of an earthquake. EDF has installed a system for reactor trip on a seismic signal, using four seismic sensors already installed on the external walls of reactor buildings, triggering a reactor trip if acceleration exceeds 0.1 g on at least two sensors;
- residual heat removal from the core by the hardened safety core while the reactor is at power will give priority to using the steam generators for this purpose. EDF did not initially choose this option, only considering the feed-and-

bleed operating mode for cooling. This type of procedure, however, involves deliberately opening the reactor coolant system, entailing a risk of containment bypass because it is necessary to recirculate water. After discussions with IRSN and obtaining the opinion of the Advisory Committee for Reactors, EDF recognized the advantage of using the steam generators. To ensure the reliability of this function in the beyond-design-basis hazard cases, EDF decided to reinforce the steam generator feedwater system, designed to withstand such hazards. Using this system, the residual heat of the reactor coolant system can be removed to outside the containment, thereby limiting the pressure increase in the containment;

- to avert containment integrity failure in the event of core melt in 900 MWe, 1300 MWe and 1450 MWe reactors, a dedicated system for removing heat from the containment will be installed (an ultimate containment spray system, CSSu). The capacity of the containment penetrations to withstand beyond-design-basis hazards will be verified and reinforced if necessary. The hydrogen recombiners are part of the hardened safety core;
- for the Flamanville 3 EPR, all the core-melt situation mitigation measures are integrated into the hardened safety core: for example, this is the case of the containment heat removal system (CHRS), which transfers heat produced in the containment from the reactor to the ultimate heat sink through the component cooling water system (CCWS) (see Section 18.2.3).

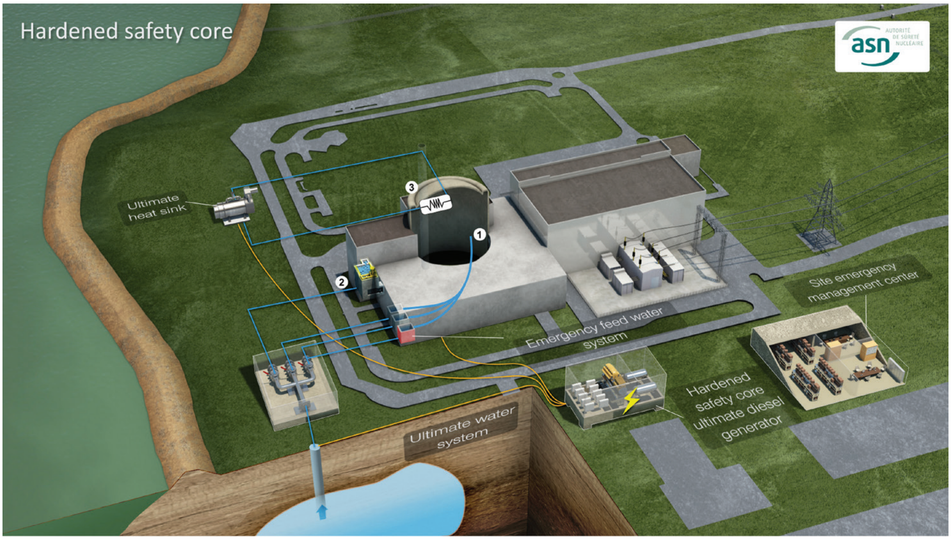
Proper implementation of the residual heat removal systems requires new water reserves, pipes, pumps, power supplies and instrumentation and control systems. This includes the ultimate diesel generators (UDG) mentioned above, for example, designed to withstand beyond-design-basis hazards.

For the Flamanville 3 EPR, the 'station blackout' (SBO) diesel generators will serve as the ultimate diesel generators (Section 18.2.3). They will be able to power two motor-driven pumps of the emergency feedwater system (trains 1 and 4) and the containment heat removal system, equipment designed to withstand the hardened safety core design-basis earthquake.

For emergency response management, EDF plans to build, on each site, a local emergency operation centre capable of withstanding beyond-design-basis natural hazards; it will house the emergency response management centre forming part of the post-Fukushima hardened safety core consisting of equipment, organizational and human resource measures. The local emergency operation centre will allow personnel to remain on the site even when the state of plant systems is highly degraded.

In addition to equipment measures, the capacity of the hardened safety core to cope with a 'hardened safety core situation', for example in the case of an extreme hazard, depends on the capacity of organizational and human resources to manage the situation. For this purpose, the following must be ensured:

- availability of reliable information on the state of the plant systems and their environment,
- availability of appropriate human resources (in terms of numbers, skills, etc.) for implementation of the hardened safety core and taking decisions on both control of the plant systems and protection of personnel on site,
- availability of procedures (operating strategies, severe accident operating guidelines) appropriate for the extreme conditions that would have to be faced by the shift crews, and effective logistic resources.


Hardened safety core
asn AUTORITÉ DE SÛRETÉ NUCLÉAIRE
Ultimate heat sink
3
1
2
Site emergency management center
Emergency feed water system
Hardened safety core ultimate diesel generator
Ultimate water system

January 2014

1 : reactor cooling system
2 : fuel pool cooling system
3 : reactor containment cooling system

Figure 36.12. Schematic diagram of the hardened safety core principle for French nuclear power reactor units.

▶ Spent fuel pools

Lessons were also learned from the Fukushima Daiichi nuclear power plant accident regarding the safety of spent fuel pools. These aspects are discussed in detail in Section 15.4.

36.6.6. Nuclear Rapid Response Force (FARN)

EDF conceived the FARN force to provide external support (Figure 36.13) to a facility in a difficult situation:

- its mission is to provide assistance as needed to any site where an accident occurs by supplying human resources, equipment (lighting, air compressors, pumps, etc.) and supplies (fuel for diesel generators, water, etc.);
- it must deploy the first-response units on site within 24 h;
- the resources provided must be sufficient to allow first-response action to be taken even when infrastructure (including site access) has suffered major damage, in radiological or toxic conditions requiring specific equipment (four-wheel drive vehicles, helicopter, protective equipment against ionizing radiation or toxic substances, etc.).

A national reconnaissance team would first be sent to the accident site within about 12 h after the decision to engage FARN resources. This advance team would assess the situation at the site and its needs in terms of off-site relief measures, and define the location of a 'rear base' operating 20 to 30 km from the site. Several potential base locations have been designated in advance for each site. When an accident occurs, the rear base is installed at the most suitable location given the actual accident situation.

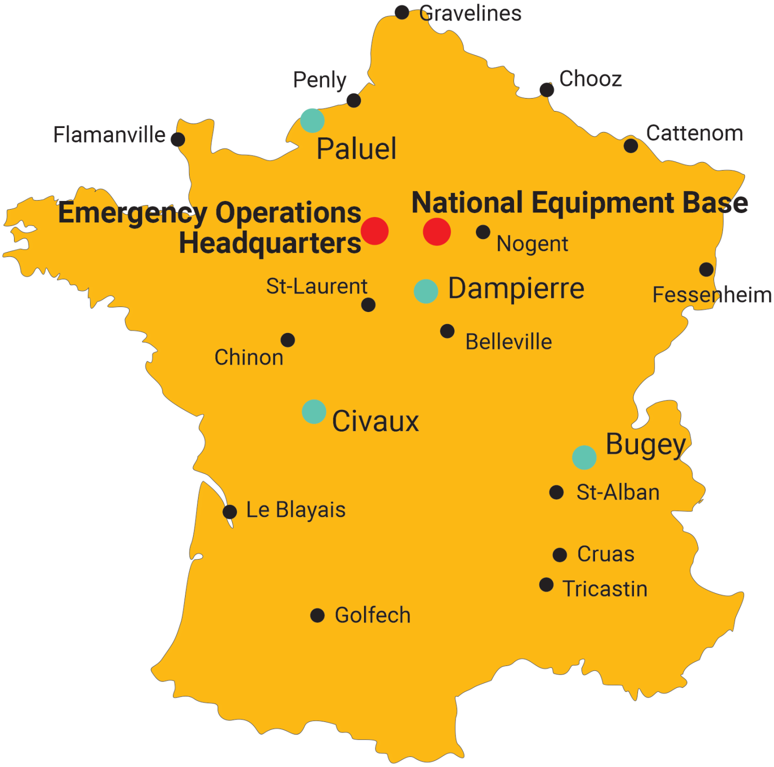


Figure 36.13. The FARN response plan is based on a three-level organization: local (black), regional (green), national (red). IRSN (source EDF).

One or more detachments of the regional teams based at the Civaux, Paluel, Dampierre-en-Burly and Bugey sites (five detachments of about 10 people at each regional base) would then be sent to the site to assist with facility control and engage mobile equipment to restore facility power or water supplies; for this purpose, standard connection points are provided in the power plants. Within three or four days, heavy equipment could be transported to the site, so that on-site teams can organize longer-term management of the situation (water supply, effluent and waste treatment, etc.).

The FARN plan provides means to supply water (tanks, pumps and filtration systems), electrical power and compressed air, as well as instrumentation and control systems and lighting equipment. It also has means to ensure logistics, operations and communications. The FARN teams are specially trained for working in a highly degraded environment.

The FARN plan has been operational since the end of 2015.

36.6.7. Deployment of post-Fukushima measures in French nuclear power plants

Given the magnitude of the changes to be incorporated in French nuclear power plants following the Fukushima Daiichi nuclear power plant accident and the number of facilities concerned, EDF decided to deploy the hardened safety core for the 900 MWe [excluding Fessenheim], 1300 MWe and 1450 MWe reactors in three phases:

– **Phase 1** – now completed – mainly aimed to reinforce reactor robustness with regard to situations involving total loss of power supplies or loss of cooling (heat sink). The measures implemented were intended to cope with such situations for longer durations than those defined previously, and also considered situations in which all the reactor units in a plant were affected. For example, an emergency diesel generator (pending the ultimate diesel generator) was installed for each reactor unit so that, in a total loss of power situation, power could be restored to part of the instrumentation and control system, control room lighting, and certain sensors (pressure in the containment or water level in the spent fuel pool, for example); the generator could also supply emergency power to certain equipment items essential for managing the situation.

  In parallel, the FARN plan was established. Some 300 people have been assigned to this team[972]; their training, started in 2012, planned to last eight years, aims to instruct responders so that they are operational in high-stress, extreme situations. Simulation exercises, based on proven examples of training and preparation measures implemented within civil defence and armed forces, are held to test organization and deployment of the corresponding measures. Taps are installed on existing systems for connection of mobile supply equipment, for

[972] Mainly from the nuclear power plant fleet. This number has been calculated to mobilize four on-call teams 24 h a day, seven days a week, ready to respond on at least three pairs of reactor units.

example to feed water to the steam generators or makeup water to a spent fuel pool, or to supply compressed air to pneumatic valves.

Facility on-site emergency plans have been reinforced to improve the response to an accident affecting all the reactor units at a given site and to prepare for deployment of the FARN team. Earthquake resistance of the emergency response rooms has also been reinforced, pending construction of the local operating centre planned in Phase 2.

- **Phase 2** – from 2017 to 2021 – covers incorporation of the first elements of the hardened safety core, which will supplement the measures implemented in Phase 1. It includes on-site implementation of measures required to respond to more severe hazards than those taken into account in the facility design phase. Each reactor unit will have an ultimate diesel generator (UDG) capable of powering all the hardened safety core equipment. On completion of Phase 2, the UDGs will also be able to restore the electrical power supply to the existing engineered safety features. The installation of a dedicated 'ultimate' heat sink (HSu), different from the initial heat sink and protected against the hazards defined for the hardened safety core design, which would be used to cool the reactors and pools, is also planned. Depending on the site, this heat sink will be supplied by pumping groundwater or by pumping water from existing basins or new water reserves.
- **Phase 3** – programmed from 2019 to some time in the 2030s, depending on the reactor units and their ten-yearly inspection programme – will cover installation of the last hardened safety core equipment, for example reinforcement of the steam generator feedwater system, which could also be supplied with electricity from the ultimate diesel generator and with water from the HSu dedicated heat sink. It should be noted that, as part of Phase 3 and among the other improvements planned for the fourth ten-yearly reactor outage (see Section 30.5), the ultimate containment spray system (CSSu) discussed in Section 36.6.5, in association with the ultimate diesel generator (UDG) and the ultimate heat sink (HSu), will be operational; in the event of core melt, it will ensure removal of heat released in the containment, with a view to maintaining containment integrity as much as possible (without filtered venting).

36.7. Other lessons learned in France from the Fukushima Daiichi nuclear power plant accident

The practical measures adopted rapidly in France have been described extensively in the sections above. Discussions nonetheless continue on various subjects, such as the safety approach that has been applied until today. In this regard, taking into account external hazards of greater magnitude than those considered in the design-basis conditions was included in ASN Guide No. 22, issued in 2017, giving recommendations for pressurized water reactor design; such hazards must now be considered in the design extension conditions (DEC). This topic is discussed further in Section 12.1. Furthermore, studies and research have been undertaken in human and social sciences on risk governance, as demonstrated by the AGORAS[973] project.

Videos available for viewing

Analysis by IRSN of the Fukushima Daiichi Accident of March 2011

Understanding the Fukushima Daiichi Accident

Environmental Impact of the Fukushima Daiichi Accident

Fukushima: Post-accident Health Issues

[973] These actions are not discussed here; for further information, refer to the IRSN publication Current State of Research on Pressurized Water Reactor Safety, J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017.

Chapter 37

Lessons Learned from the Fukushima Daiichi Nuclear Power Plant Accident: Work Conducted by the IAEA and WENRA, Action Taken in Countries Other than France

The Fukushima Daiichi nuclear power plant accident led to considerable efforts to learn as much as possible from this event. This chapter takes a brief look at work accomplished by the International Atomic Energy Agency (IAEA) and the Western European Nuclear Safety Regulators Association (WENRA), followed by lessons learned from the accident in a few countries other than France[974]. Obviously it is not possible for this book to cover every country that operates nuclear power reactors; besides Japan, only the USA and Belgium (as a European Union country different from France) are discussed here.

After the Fukushima Daiichi nuclear power plant accident and following the stress tests carried out by the different EU countries in response to the European Council's decision, Germany permanently shut down seven of its oldest reactors and began the process of phasing out nuclear power by 2022; at the end of 2019, it still had

[974] The measures taken by the international association WANO after the accident are explained in Section 3.1.5.

seven reactors in operation (one boiling water reactor and seven pressurized water reactors – including two 'KONVOI' reactors).

In the case of Switzerland, five reactors were in operation (two boiling water reactors and three pressurized water reactors). In 2011, after the Fukushima Daiichi nuclear power plant accident, the Federal Council and the Parliament took the decision in principle to gradually phase out nuclear power, choosing to shut down reactors once they reached 50 years of operation[975], i.e. between 2019 and 2034, without replacing them with new nuclear power plants. On 27 November 2016, Swiss citizens rejected the popular initiative Phase Out Nuclear Power, which aimed to ban the construction of any new nuclear power plants in Switzerland and restrict the operating lifetime of the five existing reactors to 45 years – which would have led to the immediate shutdown of the two units at the Beznau nuclear power plant, commissioned in 1969 and 1971. The Federal Council and the Parliament had recommended rejection of this initiative because it would have led to what was considered to be a premature shutdown of the nuclear reactors. The 2011 decision is part of the Energy Strategy 2050 developed in 2016 and gives Switzerland time to reform its energy supply. The Swiss power utility BKW Energie SA did announce, however, the permanent shutdown of its Mühleberg nuclear power plant by 20 December 2019, because the cost of addressing compliance gaps in certain equipment items affected by anomalies was too high (the plant was shut down on the planned date).

37.1. Work conducted by the IAEA

After the Fukushima Daiichi nuclear power plant accident, the IAEA drew up an action plan (IAEA Action Plan on Nuclear Safety), which was approved by its Board of Governors at a meeting on 13 September 2011. The plan, covering 12 topics, implemented a series of actions, including three of particular note:

- encouraging Member States to undertake safety assessments of their nuclear facilities in light of events at the Fukushima Daiichi nuclear power plant,
- encouraging Member States to conduct assessments of the role and effectiveness of their safety regulators,
- launching a review of IAEA standards, based on a work programme that set priorities, and revising these standards as necessary.

In 2015, the IAEA issued a dossier entitled The Fukushima Daiichi Accident, consisting of a summary report by the IAEA's Director General and five volumes written by a large number of experts. The main topics covered in the dossier include the following:

- description and background of the accident,

[975] The five Swiss nuclear reactors in question were commissioned between 1969 and 1984 (Beznau Unit 1, Beznau Unit 2, Mühleberg, Gösgen and Leibstadt). The operating licences for these reactors have no time limit, which means they can continue to operate as long as they are considered safe.

- safety aspects,
- management of the accident and aspects of emergency preparedness and response,
- radiological consequences of the accident,
- post-accident recovery of contaminated land.

With regard to the radiological consequences of the Fukushima Daiichi nuclear power plant accident, the IAEA dossier is based particularly on reports by international bodies such as the WHO and UNSCEAR (see Section 36.5 in the previous chapter), as well as the ICRP, which carried out a review of radiation protection aspects during and after the accident with a view to improving the international radiation protection system (the ICRP's report was issued in 2012).

In its dossier, the IAEA highlights the fact that at the Fukushima Daiichi nuclear power plant, the flooding caused by the tsunami simultaneously affected the first three levels of defence in depth, leading to common-cause failures of equipment and systems. The IAEA considers that, while the principles of the defence-in-depth concept remain valid, its application must be reinforced at all levels through independence, redundancy, diversity and protection from both internal and external hazards, while focusing on accident prevention as well as improving risk mitigation measures. Taking into account external events of a larger scale than those used as the design basis for facilities also appeared to be necessary.

The IAEA's plan also included a programme to revise its standards. Discussions on priorities identified that five of these required immediate attention:

- GSR Part-1: Governmental, Legal and Regulatory Framework for Safety,
- NS-R-3: Site Evaluation for Nuclear Installations,
- SSR-2/1: Safety of Nuclear Power Plants: Design,
- SR-2/2: Safety of Nuclear Power Plants: Commissioning and Operation,
- GSR Part-4: Safety Assessment for Facilities and Activities.

The revised standard SSR-2/1 (Safety of Nuclear Power Plants: Design), issued in 2016, places particular emphasis on taking into account hazards, by considering more severe events than those covered during a simple site assessment, while giving greater attention, more generally, to extreme events that could simultaneously affect several units at a given site, and considering, from the design stage, the benefits of installing connecting fixtures for mobile emergency equipment, etc.

37.2. Work conducted by WENRA

As explained previously in Chapter 36, WENRA responded in April 2011 to the European Council's request of March 2011 by preparing and proposing specifications for stress tests to be carried out in EU countries.

In light of lessons learned from the Fukushima Daiichi nuclear power plant accident, WENRA subsequently decided to carry out a review of the 'reference levels' it had drawn up in 2006 for existing nuclear power plants (revised in 2007 and 2008 – see Section 6.6). Its Reactor Harmonisation Working Group (RHWG) carried out this review taking into account not only the recommendations and suggestions put forward by ENSREG following the stress tests and the revised IAEA standards, but also initiatives taken by each WENRA member in terms of changes to national legislation following the Fukushima Daiichi nuclear power plant accident. This work was also inspired by the working group's initial reflections on lessons to be learned from the accident, which the working group had published in its 2013 report Safety of New NPP Designs, dedicated to new reactors.

This work led to the adoption by WENRA and the publication in September 2014 of the report entitled WENRA Reference Levels for Existing Reactors/Update in Relation to Lessons Learned from TEPCO Fukushima Daiichi Accident. The development of these reference levels was the fruit of prior consultation with stakeholders.

The main changes compared to the old reference levels involved the Issue F section, Design Extension of Existing Reactors, which was completely rewritten, and the Issue T section, Natural Hazards, which was entirely new. Substantial changes were also made to Issue LM, Emergency Operating Procedures and Severe Accident Management Guidelines and Issue R, On-site Emergency Preparedness.

The changes and additions were mainly designed to ensure better coverage of events affecting several units at a given site, including reactors and spent fuel pools, as well as the possibility of more severe conditions occurring than those taken into account in design-basis conditions.

37.3. Japan

In his introductory message to the report by the independent investigation commission set up by the Japanese parliament on the Fukushima Daiichi nuclear power plant accident, the commission chairman, K. Kurokawa, listed a number of societal factors that, according to the commission, contributed to an accident 'that could have been foreseen'.

The concrete measures rapidly taken by Japan after the accident concerning the nation's nuclear power plants were explained in the previous chapter (Section 36.6).

From the more general perspective of controlling safety[976], the Fukushima Daiichi nuclear power plant accident led to the dissolution of the Nuclear and Industrial Safety Agency (NISA), a subdivision of the Ministry of Economy, Trade and Industry (METI). This agency (see Figure 37.1) was criticised, particularly in the aftermath of the accident, because of conflicts of interest within METI, which was also in charge of the

[976] For more on this subject, refer to the historical account written by Hideaki Shiroyama, entitled Nuclear Safety Regulation in Japan and Impacts of the Fukushima Daiichi Accident.

nuclear industry. Moreover, the distribution of roles and responsibilities between NISA and another body, the Nuclear Safety Commission (NSC), which reported to the Prime Minister and acted as a joint regulator, seemed unclear. Apart from NISA, it was considered that the general organization and the multiplicity of the various safety bodies involved at the time of the Fukushima Daiichi nuclear power plant accident had caused delays in decision-making. On 20 June 2012, the Japanese government abolished NISA and the NSC and replaced them the following September with a nuclear regulatory authority, the NRA (Nuclear Regulation Authority), which reported to the Ministry of the Environment (MOE) and was led by a chairman and four commissioners. Then, in 2014, the NRA was strengthened by merging with its main technical support organization, the Japanese Nuclear Energy Safety Organisation (JNES), taking on its staff of about 400 people; this approximately doubled the NRA's human resources. This merger marked a step towards Japan's goal of grouping resources and combining the different bodies involved in controlling nuclear safety.

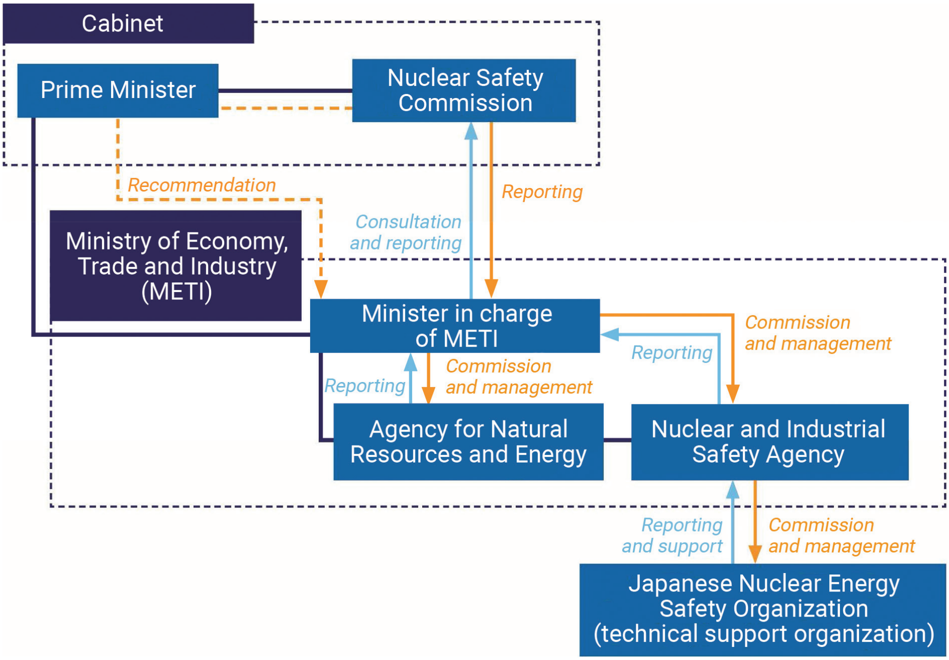

Cabinet
Prime Minister
Nuclear Safety Commission
Recommendation
Reporting
Consultation and reporting
Ministry of Economy, Trade and Industry (METI)
Minister in charge of METI
Commission and management
Reporting
Reporting
Commission and management
Agency for Natural Resources and Energy
Nuclear and Industrial Safety Agency
Reporting and support
Commission and management
Japanese Nuclear Energy Safety Organization (technical support organization)

Figure 37.1. NISA's place in the Japanese administration before the Fukushima Daiichi nuclear power plant accident. IAEA (source: The Fukushima Daiichi Accident).

37.4. Belgium[977]

37.4.1. Nuclear power plants in Belgium

In Belgium, seven pressurized water reactors are operated for nuclear power generation by electricity producer ENGIE Electrabel on two separate sites:

- four reactors on the Doel site near Antwerp (Flanders), beside the Scheldt River:
  - Doel units 1 and 2 are twin units of 433 MWe each, commissioned in 1975,
  - Doel Unit 3 is a 1006 MWe unit commissioned in 1982,
  - Doel Unit 4 is a 1039 MWe unit commissioned in 1985;
- three reactors on the Tihange site near Liège (Wallonia), beside the Meuse River:
  - Tihange Unit 1 is a 962 MWe unit commissioned in 1975,
  - Tihange Unit 2 is a 1008 MWe unit commissioned in 1983,
  - Tihange Unit 3 is a 1054 MWe unit commissioned in 1985.

For all nuclear safety-related aspects, the operators' activities are controlled by:

- the Federal Agency for Nuclear Control (AFCN, www.fanc.fgov.be/fr),
- Bel V, its technical subsidiary (www.belv.be).

37.4.2. General details on the design of Belgian nuclear power plants

The four most recent units have an important feature as regards the lessons to be learned from the Fukushima Daiichi nuclear power plant accident: external hazards (whether natural or induced by human activities) were taken into account from the facility design phase according to a special approach. In addition to the 'first level of protection' consisting of the usual systems, these units were given a 'second level of protection'. This second level of protection protects against hazards of external origin (particularly those resulting from human activities such as aeroplane crashes, external explosions, a large-scale fire). Accordingly, the buildings and systems that form part of this second level of protection are designed to withstand these hazards and remain operational after the event. For several safety aspects, this second level of protection introduces redundancy and diversity with regard to the first level of protection. This is the case, for example, with the feedwater supply to the steam generators, the electrical power supplies, and maintaining the integrity of the reactor coolant pump seals.

[977] This section was written by Marc Vincke and Pieter de Gelder, from the Belgian organization Bel V.

When the three oldest units were designed, regulations were not as complete, so changes were made later (during the ten-yearly reactor outages) to improve protection against hazards of external origin.

Core-melt accidents were not taken into consideration during the design phase of any nuclear power plants in Belgium. Once again, during the ten-yearly outages, changes were made to improve protection against these accidents. For example, all nuclear power plants have been fitted with passive autocatalytic recombiners in their reactor buildings to prevent hydrogen explosions that could jeopardize reactor containment integrity.

37.4.3. Stress tests and main lessons learned

As in other European countries, the operator of Belgium's nuclear power plants carried out stress tests in 2011 to assess its facilities' response to different extreme scenarios. This resulted in an action plan of improvements[978], some of which were implemented as early as 2012.

The units on which the stress tests were carried out were the seven reactors listed above, and associated systems such as the spent fuel pools[979].

Some of the main aspects of the assessments performed and the improvements chosen following the stress tests on the nuclear reactors are explained in more detail below. Details specific to the different nuclear power plants and information on the progress of the action plan come from publications of the Belgian nuclear safety regulator[980].

37.4.3.1. Improving protection of facilities against external hazards

The external hazards taken into account in the stress tests were earthquakes, flooding and meteorological phenomena, including extreme weather events.

In Belgium, an average return period of 10,000 years was used to assess and improve design in the case of earthquakes and external floods; the same value was used as the target for meteorological phenomena, where available data allowed.

▶ Earthquakes

To determine whether the earthquake criteria used in the design basis for a reactor were sufficient, a preliminary probabilistic assessment of seismic risk was carried out during the stress tests. At the request of the Belgian nuclear safety regulator, a more in-depth assessment has been carried out since then. The results, approved by the

[978] BEST, for BElgian Stress Tests.

[979] Similar stress tests were also carried out at Belgian nuclear facilities other than nuclear power plants.

[980] Since 2012, the Belgian nuclear safety regulator has published various updated reports on the subject; for example, the March 2019 version can be accessed from the following link: https://afcn.fgov.be/fr/system/files/2019-03-11-best-2018-final.pdf.

regulator, allowed the operator to confirm that the design-basis earthquake criteria used for the Doel and Tihange sites were adequate.

As part of the stress tests and the assessment of seismic margins, a significantly higher level of extreme earthquake (up to 1.7 times higher in terms of maximum ground acceleration) than the reactor design-basis earthquake was adopted. This assessment showed that the structures, systems and components necessary to reach and maintain a safe shutdown state had a sufficient probability of withstanding the postulated earthquake conditions, except for a few items of mechanical and electrical equipment requiring further demonstrations and, where appropriate, corrective action, which have all been implemented.

▶ External flooding

As regards the risk of external flooding, the Doel plant has the advantage of being located at a high elevation. The stress tests did not cast doubt on the adequacy of the design of the site's protection against this risk. A few extra measures, such as protective barriers at the entrance to buildings containing equipment important to safety, were nevertheless implemented following the tests.

The ten-yearly reactor outage at the Tihange site in progress before the Fukushima Daiichi nuclear power plant accident showed – based on a probabilistic approach – that the site was not adequately protected against external flooding risks: the average return period of the reference flood was between 100 and 1000 years, well below the target value. Accordingly, in 2011 the operator decided to significantly improve the site protection measures.

The stress tests led to the reinforcement and acceleration of this improvement process; the following measures are now operational:

1. Peripheral protection of the site (see Figure 37.2) corresponding to an updated reference flood with a sufficiently long average return period, consisting of a wall, isolation devices at water inlets, cooling water discharges and outlets into the Meuse River.

2. Additional permanently installed equipment for each unit (a 6 kV diesel generator housed in a special building, pumps to supply groundwater to make up water levels in the steam generators, the spent fuel pools and the reactor coolant system, etc.); this equipment is installed at least one metre above the updated reference flood level and would suffice if the peripheral protection failed or if there was extreme flooding that went beyond the design basis of the peripheral protection.

3. Improvement and adaptation of the on-site emergency plan strategy and organization, and in particular, at the Belgian nuclear safety regulator's request, of the flood pre-alert and alert system, based on a signed agreement for more effective communication with the regional flood protection authority and access to water flow rate and level measurements for the Meuse River.

4. Measures to protect against the risks that could result from flooding inside a facility (caused by a fire or an explosion), at the request of the Belgian nuclear safety regulator.

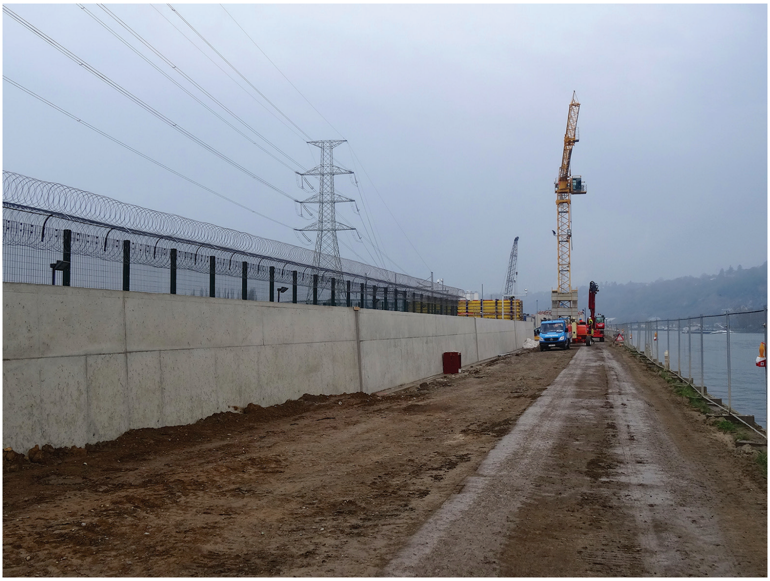


Figure 37.2. Peripheral protection of the Tihange site. Tihange nuclear power plant.

▶ Extreme weather phenomena

The stress tests led to action to reinforce the protection of sites and their units against risks from heavy rain, tornadoes, snow and lightning.

In particular, the Belgian nuclear safety regulator asked the operator to assess the ability of water drainage systems on the Doel and Tihange sites to cope with short periods of heavy rain and periods of long-term rain defined using data that takes into account a 1000-year return period with a high degree of confidence.

At Doel, the assessment showed that the site was adequately protected against the risk associated with heavy rain. At Tihange, the internal flooding risk on the site due to overflow of the water drainage system led to major improvements consisting mainly of diverting the municipal culvert that originally crossed the site (see Figure 37.3) into the Meuse upstream of the site, and modifying the drainage outlets from the site sewers into the Meuse. The need for additional improvements to ensure adequate protection of the site against the risks associated with heavy rain was then assessed, and inspection campaigns and maintenance of the water drainage systems were recommended.

Figure 37.3. Diverting the municipal culvert upstream of the Tihange site. Tihange nuclear power plant.

37.4.3.2. Improving protection of facilities against loss of electrical power supplies or loss of heat sink

In Belgium, before the Fukushima Daiichi nuclear power plant accident, nuclear power plants had diversified electrical power supplies and cooling water sources. For example, in addition to redundant off-site power supplies, emergency diesel generators (and the water in rivers), these included:

- the water stored in different tanks on both sites, and the groundwater or water in artificial pools and lakes,
- air cooling of certain equipment (heat exchangers, forced-draught cooling towers, diesel generators),
- the turbine-driven pump of the auxiliary feedwater system (in the first level of protection) provided for each reactor.

Cooling of reactor cores and spent fuel pools could therefore be guaranteed in different situations of partial loss of power supply or heat sink with an autonomy typically of several weeks.

The stress tests prompted the decision to protect Belgian reactors against situations with even lower probabilities, such as total loss of power supplies (aggravated by the assumption of a larger earthquake than the one used as the design basis) and total loss of heat sink. This decision led to the implementation of strategies based on procedures and resources that would prevent a core-melt accident in these situations, which are now operational. Some aspects of these strategies are generic (such as improvements to ensure availability of reliable spent fuel pool water level measurements in the situations to be covered), while other aspects of these strategies differ depending on specific conditions.

The strategy developed for the Doel site is based on the use of mobile diesel generators and mobile pumps, stored in a specially built storage building that can withstand the external hazards taken into account in the stress tests. A new multi-function fire truck can also serve as a mobile pump. The mobile diesel generators can be connected to existing 380 V electrical switchboards to supply the existing safety equipment essential to the strategies implemented (instrumentation and control, compressors, valves). In this strategy, the mobile pumps can be used at each unit to supply water from artificial ponds to the emergency feedwater system (second level of protection), the reactor coolant system, the containment spray system and the spent fuel pools, through hoses and connection points to fixed pipes.

The strategy developed for the Tihange site is based mainly on the use of existing or new, permanently installed equipment. In each unit concerned, a new 6 kV diesel generator housed in a special building (also provided as protection against external flooding risks) is connected to existing 6 kV electrical switchboards to supply power to existing safety equipment essential for the strategies implemented (pumps, instrumentation and control, compressors, valves) through an additional permanently installed 6 kV system (with switchboards, cables and circuit breakers). The existing pumps powered in this way can supply groundwater to the steam generators and spent fuel pool cooling systems, as well as makeup water to the reactor coolant system from existing borated water tanks. The exact solutions (choice of systems, pumps and tanks) vary from one unit to another. In a situation of total loss of heat sink, the many tanks available would provide the necessary water for the strategy instead of the groundwater, which is assumed to be lost. Specific design features (such as the closed safety position of most compressed air valves on the turbine-driven emergency feedwater pump) may require specific measures (such as, for the example mentioned above, the installation of a new, permanently installed compressed air tank to supply the existing compressed air system in the short term).

37.4.3.3. Improving on-site emergency plans

The operator’s on-site emergency plans were initially designed to manage a design-basis event affecting only one unit. During the stress tests, the operator decided that it was necessary to extend this organization to the management of beyond-design-basis events potentially affecting multiple units on the same site. The resulting adaptation of the organization (central support unit for two sites, new roles, documentation) in particular incorporated new logistic resources (additional emergency infrastructure housed in a mobile truck that can be deployed during an event to one of the two sites, calls to external contractors), the improvement and diversification of means of communication, additional means of measuring and calculating radionuclide dispersion, better management of the storage of radiation protection equipment, additional resources facilitating a response on a contaminated site, and harmonization of emergency plan exercises between sites.

37.4.3.4. Improving management of core-melt accidents

The stress tests involved a reassessment of the scenarios leading to core-melt accidents. They led to the identification of actions that would further mitigate the potential radiological consequences. Of these, the main measure decided on this occasion was the installation of filtered vents at all Belgian units (see Figure 37.4). The purpose of the filtered vents is to protect the containment, through one or more successive ventings, against the risk of a rupture associated with the core-melt accident scenarios leading to an increase in its internal pressure, and to mitigate the radiological consequences of any venting by means of filtration.

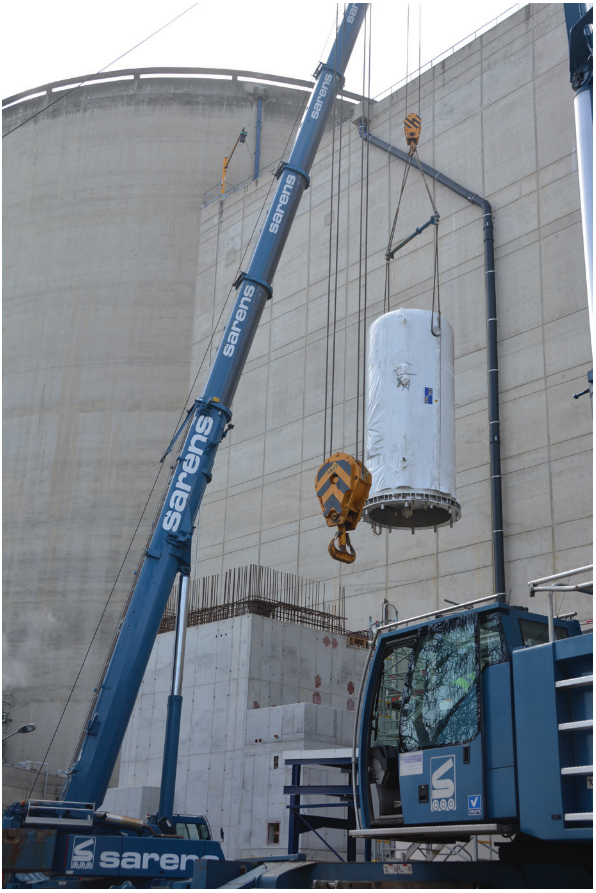


Figure 37.4. Installing the filter in Tihange Unit 3. Tihange nuclear power plant.

37.5. USA

The USA (2020 situation[981]) has a nuclear power plant fleet of 97 light water reactors units in operation, consisting of 65 pressurized water reactors (PWRs) and 32 boiling water reactors (BWRs).

Two aspects of operating experience feedback acted upon in the USA following the Fukushima Daiichi nuclear power plant accident are explained briefly below[982]; one concerns US regulations on nuclear safety, the other concerns the FLEX initiative taken by operators, featuring aspects similar to EDF's FARN initiative for the French nuclear power plant fleet.

▶ Reflections and actions regarding US regulations

On 12 July 2011, the U.S. NRC, the USA's nuclear safety regulator, published a document entitled Recommendations for Enhancing Reactor Safety in the 21st Century. This report presents a preliminary analysis carried out by the Near-Term Task Force (NTTF) set up in the aftermath of the Fukushima Daiichi nuclear power plant accident. The analysis aimed to rapidly identify any need for improvement of US regulations in light of the accident and to make recommendations to the U.S. NRC.

Since the 1980s, the US approach to nuclear power plant safety had been based on a set of events to be considered during reactor design (Design-Basis Accidents, DBA) with additional elements for events beyond the design basis (Beyond-Design-Basis Accidents, BDBA). Although no periodic safety reviews like those in other countries, such as France, were carried out, an approach aimed at improving plant safety was adopted as and when new issues arose[983]; Section 30.6.1 of this document mentions the generic issues dealt with over time.

The Task Force's analysis reviewed the U.S. NRC's entire regulatory framework; however, given the fact that the Fukushima Daiichi nuclear power plant accident had been caused by extreme natural events (on a much larger scale than those used in the design basis), the analysis focused particularly on how US regulations addressed the protection of facilities from natural phenomena and how beyond-design-basis events were addressed by the U.S. NRC.

The conclusions of the analysis identified the following key points:

- natural events are taken into account in the design of nuclear power plants in regulation 10 CFR[984] Part 50 Appendix A; during the operating lifetime of these plants, the U.S. NRC may decide to publish different types of documents on taking into account the risks associated with natural hazards, for example, in

[981] Source: Wikipedia, Nuclear Power in the USA.

[982] Numerous documents and information sources have been made public on websites.

[983] See the IAEA document Periodic Safety Review of Nuclear Power Plants: Experience of Member States, Appendix IV, Alternative Approach to PSR, IAEA-TECDOC-1643, 2010.

[984] Code of Federal Regulations.

the form of Unresolved Safety Issues (as in 1980 on earthquake qualification of certain electrical equipment items), Generic Safety Issues (as in August 2010 on taking into account flooding as a result of dam failure), Regulatory Guides explaining how to meet regulatory requirements on certain specific subjects, and other publications. The response to these recommendations is variable, since operators are not obliged, once their facilities have been commissioned, to send the results of their analyses to the U.S. NRC, so there are significant differences between facilities in how they take into account natural external hazards, particularly depending on the commissioning date of the facilities;

– requirements in terms of the beyond-design-basis events to be considered are set out in certain specific cases in special documents; this is the case, for example with station blackout[985] (SBO) for four to eight hours (rule 10 CFR 50.63);

– for reactors that were already in operation in 2011, taking measures relevant to emergency response to severe accidents is left to the operators' initiative and any documents issued for this purpose do not require review by the U.S. NRC; for new reactors, requirements have been stipulated in rules 10 CFR 52.47 (2009) and 10 CFR 52.79 (2011).

The way various issues are handled therefore appears to be quite different in terms of the types of requirements, how operators meet them and any subsequent analysis by the U.S. NRC. After observing this inconsistency, the Task Force considered that the structure of the US regulatory corpus needed improvement.

Concerning BDBAs, the Task Force insisted on the fact that an approach should be taken, possibly based on probabilistic elements, to better cope with situations that were very improbable, but likely to lead to significant radiological consequences.

Aiming to reinforce defence in depth, the Task Force made 12 recommendations that would upgrade the US regulatory framework, especially with regard to events that could be caused by natural hazards, as well as accident mitigation and emergency preparedness.

From a general perspective, the Task Force recommended:

– clarifying the regulatory framework,

– increasing surveillance of operators' ability to maintain safety at their facilities, with a particular focus on the requirements associated with implementing the defence-in-depth concept.

From a technical viewpoint, the Task Force made the following recommendations:

Ensuring facility protection

1. Require that operators reassess the earthquakes and floods used in the facility design basis and increase facility protective measures consequently (Figure 35.5

[985] This situation corresponds to the loss of off-site power sources and the main diesel generators. Batteries and other generators are assumed to be available.

shows a major flood that occurred in 2011 on the site of a US nuclear power plant).

2. In the longer term, evaluate ways to improve measures taken to prevent or mitigate fires and floods induced by earthquakes.

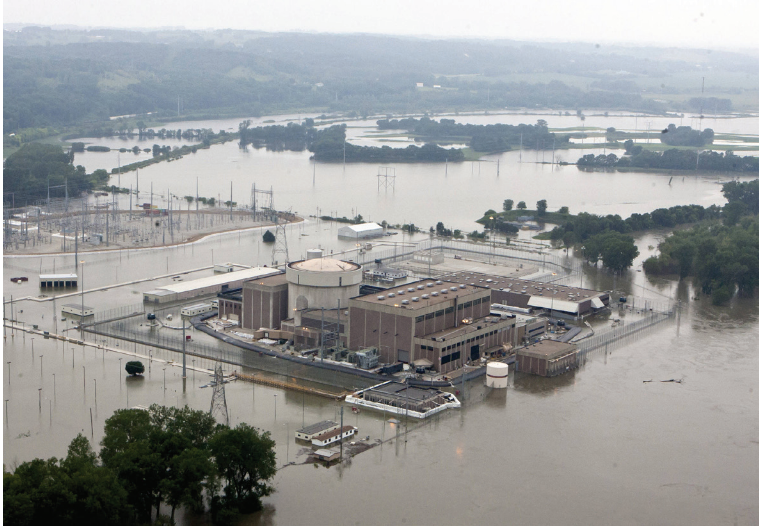


Figure 37.5. In June 2011, high river levels in Missouri caused flooding at the Fort Calhoun nuclear power plant in the USA. Nati Harnik/AP/SIPA.

Enhancing accident mitigation measures

3. Strengthen requirements involving the ability to cope with station blackout under the external hazard conditions considered for design-basis and beyond-design-basis events.
4. Install reliable, hardened venting systems in Mark I and Mark II BWRs that remain operational even in the event of total, extended loss of electrical power supplies.
5. During U.S. NRC safety reviews planned for the long term, take into account any new knowledge on ways of monitoring the presence of hydrogen and the associated risks inside reactor buildings or other buildings, as more detailed information becomes available on events that occurred at the Fukushima Daiichi nuclear power plant.
6. Enhance spent fuel pool makeup capability and instrumentation for spent fuel pools.
7. Reinforce on-site emergency response capabilities and take them into account in emergency operating procedures, severe accident management guidelines, etc.

Reinforcing emergency preparedness

8. Take into account facility emergency plans for extended station blackout and events affecting multiple units on the same site.
9. With a view to safety reviews planned for the longer term, define additional emergency preparedness topics related to extended station blackout or events affecting multiple units on the same site.
10. For these reviews, pursue analysis of emergency response needs in terms of decision-making, radiation monitoring and educating the public living near nuclear power plants (on safety and radiation protection).

The U.S. NRC followed up these recommendations in different ways: orders or requests for information were sent to operators, changes were made to regulations, a longer-term review of topics was conducted by the U.S. NRC. Based on the Task Force proposals, the subjects to be addressed as part of the upgrading of US regulations were as follows:

- setting up periodic reassessments of the hazards to be taken into account,
- taking into account phenomena induced by these hazards (such as fires and floods),
- managing situations featuring extended loss of electrical power (such as station blackout),
- protecting containment structures from internal overpressure (by venting),
- hydrogen explosion risks,
- spent fuel pools,
- emergency response to events affecting multiple units (reactors and pools) simultaneously on the same site, particularly in the event of an extended station blackout.

In October 2011, the U.S. NRC divided these topics into three groups in decreasing order of priority, known as Tier 1, Tier 2 and Tier 3; the Tier 1 topics were to be addressed without delay. It should be noted in particular that:

- the following operations were begun as part of Tier 1: enhancing plant autonomy in the event of extended station blackout (required by order), installing robust, reliable means of venting containment structures in Mark I and Mark II boiling water reactors (by order), installing reliable instrumentation to measure the water level in spent fuel pools (by order), a reassessment of the ability of facilities to withstand earthquake and flood conditions, together with walk-downs[986] to identify and correct any weaknesses; evaluation and reinforcement, as neces-

[986] These checks are to be carried out at facilities, based, for example, on visual observations and engineer's opinions, in light of the design specifications, safety plans and safety requirements for the relevant facility. Guidelines exist on the subject, such as those published in 2012 by the Electric Power Research Institute (EPRI) and the Nuclear Energy Institute (NEI) for walk-downs to be carried out in the USA after the Fukushima Daiichi nuclear power plant accident.

sary, of emergency response means (human resources, information available to teams responding to emergencies) in the case of events affecting multiple reactors on the same site;

- the periodic (ten-yearly) reassessments of external hazards (through a change in the regulations) are mainly included in Tier 3.

In addition to the U.S. NRC, other bodies and associations have carried out or been involved in operating experience feedback in the USA following the Fukushima Daiichi nuclear power plant accident; these include the Nuclear Energy Institute (NEI) and the American Society of Mechanical Engineers (ASME), which in 2012 produced a document entitled Forging a New Nuclear Safety Construct, which includes comments on the regulatory framework governing the nuclear sector in the USA.

▶ Initiative taken by US operators: the FLEX strategy

A US industry coordination body, the Fukushima Response Steering Committee, developed the FLEX concept. This body included representatives of US electrical power utilities, the Nuclear Energy Institute (NEI), the Institute of Nuclear Operations (INPO) and the Electric Power Research Institute (EPRI). Its members worked for a year to make sure that the lessons to be learned from the Fukushima Daiichi nuclear power plant accident had been collected, understood and incorporated into the various improvement plans. In January 2012, the U.S. NRC was presented with a set of measures constituting the FLEX strategy (Diverse and Flexible Coping Strategies), to take into account the major difficulties encountered at the Fukushima Daiichi nuclear power plant, generally concerning facility electrical power supplies and cooling (heat sink). The FLEX strategy measures (see Figure 37.6), designed in response to the requirements expressed by the U.S. NRC (mainly in Tier 1), constitute a supplement to a certain number of measures implemented following the attacks on 11 September 2001 on the World Trade Center in New York.

The FLEX strategy relies on the facilities' own equipment, mobile equipment present on site and equipment stored off the site. It is specified in NEI 12-06 dated August 2012 and was judged acceptable by the U.S. NRC[987], after a few clarifications. Implementation of the corresponding measures therefore began in 2012 and was completed at the end of December 2016.

NEI 12-06 stated that each operator should decide the exact measures it would take under the FLEX strategy based on individual site and unit characteristics, particularly as regards external hazards and the corresponding levels of protection, including beyond-design-basis situations (extreme hazards); the analysis must take into account not only earthquakes and external flooding, but also hazards such as hurricanes, tornadoes and extreme temperatures.

[987] See Interim Staff Guidance JLD-ISG-2012-01 – Compliance with Order EA-12-049, Order Modifying Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events.

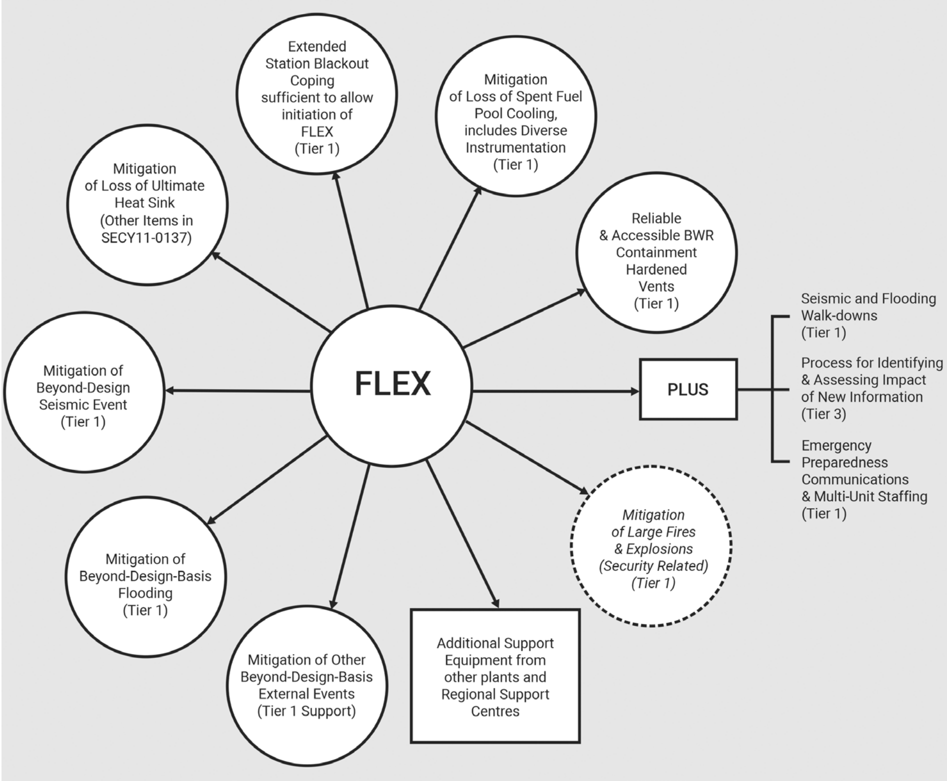


Figure 37.6. Diagram of the FLEX strategy (NEI 12-06). IRSN.

However, without delay, mobile multi-use equipment was rapidly installed in secure locations (diesel generators, batteries and battery chargers, compressors, pumps, etc.), especially at two regional centres – known as SAFER[988] Response Centers, in Memphis (Tennessee) and Phoenix (Arizona) – capable of providing support within 24 h. Each regional centre has five similar sets of equipment, four of which are in a permanent state of readiness so that, if necessary, they can be rapidly deployed to any nuclear power plant in the USA. This equipment must undergo periodic testing.

[988] Strategic Alliance for FLEX Emergency Response.

Chapter 38
Emergency Preparedness and Response

Despite measures taken during the design and operation of nuclear facilities, an accident leading to a radiological emergency situation[989] cannot be ruled out. In theory, this type of situation may concern any basic nuclear installation, and in particular, any nuclear power reactor. This is why measures are taken locally, nationally, and in some cases internationally, to respond to this situation.

Historically[990], measures were defined and implemented in the 1980s, based largely on lessons learned from the accident in 1979 at the Three Mile Island nuclear power plant in the USA and the multiple problems that arose in response to this situation concerning the entities involved, the information and instructions provided to the public, the choice of a strategy for distributing stable iodine tablets to the population, etc. While the principles of the 'emergency plans' to be used by the prefects[991] in the

[989] Or radiological emergency situations. This chapter focuses on radiological emergencies, but there are also other types of situations that may lead to implementing a local and national emergency response (toxic releases, etc.).

[990] This information is taken from Philippe Saint Raymond's work entitled *Une longue marche vers l'indépendance et la transparence – L'histoire de l'Autorité de sûreté nucléaire française* (A Long March Toward Independence and Transparency – the History of the French Nuclear Safety Authority), *La documentation française*, 2012.

[991] A prefect (*préfet*) is a local representative of the national executive branch of government, responsible for defending national interests, applying administrative measures and ensuring law enforcement in local administrative areas such as *départements* and *régions* of the Republic of France.

relevant *départements*[992] in France regarding the first units of French nuclear pressurized water reactors had just been defined, the need for operators to have 'on-site emergency plans' was clearly recognized. In response to a request from the Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*, SCSIN), Électricité de France (EDF) included preparation of the on-site emergency plan in the 'post-TMI' action plan, and national emergency response organization was structured to ultimately correspond to the situation described in this chapter.

While the actions to be taken in a radiological emergency are initially local, they could rapidly become national in scope, given the sensitivity of issues concerning environmental quality, public health, continuity of social and economic activity, and international relations.

A major radiological emergency requires setting up a global response by the national government and strong coordination between the various national and local entities and stakeholders concerned, with expansion to the international level if necessary.

The various entities involved in a radiological emergency obviously include the operators of nuclear facilities, which, in France, implies EDF, who operates the reactors in the nuclear power plant fleet. Also concerned are the prefects and mayors of the impacted cities, the French Nuclear Safety Authority (ASN) and IRSN; they all have defined roles and responsibilities.

The purpose of this chapter is to present the measures taken or planned in France at the national government level to respond to a potential radiological emergency. The roles and responsibilities of the various entities will be described, with examples pertaining specifically to nuclear power reactors.

It should be noted that this chapter only covers the first phase, called the 'emergency phase', of an accident situation. Further action may be necessary over a longer term and a broader area, as the accident in 1986 at the Chernobyl nuclear power plant in Ukraine showed, as well as the accident in 2011 at the Fukushima Daiichi nuclear power plant in Japan. In France, the Steering Committee for Management of the Post-Accident Phase[993] (*Comité directeur pour la gestion de la phase post-accidentelle*, CODIRPA), set up by ASN in 2005 at the request of the French Prime Minister, made it possible for ASN to release in 2012 the first policies and guidelines for this kind of post-accident management[994]. These initial policies cover the end of the emergency phase, called the 'transition phase', and the long-term phase. These concepts

[992] In the administrative divisions of France, the *département* is one of the three levels of government below the national level (referred to as 'territorial collectivities'), between the administrative *régions* and the *communes*. There are 96 *départements* in mainland France and five overseas. (Source: https://en.wikipedia.org/wiki/Departments_of_France).

[993] Of a nuclear accident or radiological emergency.

[994] *Éléments de doctrine pour la gestion post-accidentelle d'un accident nucléaire* (Policy Elements for Post-Accident Management of a Nuclear Accident), – ASN, 21 November 2012.

will be explained below. Following work carried out between 2014 and 2019 to take into account operating experience feedback from the Fukushima Daiichi nuclear power plant accident, CODIRPA recommended several changes to these post-accident policies, the main one being simplification of post-accident zoning, which serves as the basis for taking measures to protect the population[995].

38.1. Defining a radiological emergency and 'response' objectives

In Article L.1333-3, the French Public Health Code indicates that a radiological emergency refers to "any situation implying a source of ionizing radiation and requiring a rapid response to mitigate the severe negative consequences for public health, the environment, or property, or a risk that could lead to these types of severe negative consequences."

By definition, an emergency situation is one that requires a rapid response. This includes setting up a specific organization for the purpose of managing the situation and implementing actions to mitigate the consequences that result or could result from this situation. In practice, actions taken in an emergency aim to:

- immediately activate the response organization, which will be presented below,
- restore a controlled, stable state in the facility where the accident occurred,
- protect people, including both workers and the public, to avoid deterministic effects and reduce stochastic effects as much as possible,
- provide medical and psychological care,
- provide the public with responsive, transparent and continuous information,
- to the extent practicable, prepare for the return to normal social and economic activity,
- ensure that information is exchanged as per international and European conventions,
- prepare for managing the situation over time in its post-accident phase.

Depending on the type of accident and its kinetics, the actual emergency phase may last from a few hours to a few days and may include three periods:

- a **period in which there is a threat of release** (which does not exist in emergency response terms for accidents with fast kinetics), during which actions are implemented, mainly by the operator, to re-establish a satisfactory safety level and avoid release;

[995] See https://www.asn.fr/Informer/Actualites/L-ASN-publie-les-nouvelles-recommandations-du-Codirpa.

- a **period of radioactive releases** to the environment when this cannot be avoided; releases may last several days;
- the **period at the end of the emergency phase**, lasting a few days, which begins after the end of releases, when a controlled, stable state has been restored in the facility.

Depending on the situation, protective actions can include sheltering and listening for instructions, evacuation, ingestion of stable iodine (when nuclear reactors are involved), and restrictions on the sale and consumption of foodstuffs. In parallel, public health actions (such as traffic restrictions on public roads) and policing actions are initiated. Actions to protect the population are conducted differently depending on the type of accident:

- during an accident with fast kinetics, releases may occur very rapidly (and be short-lived[996]). In this case, 'reflex mode' sheltering may be initiated by the operator, but in the conditions planned for in advance and with the agreement of the prefect for the relevant *département*;
- during an accident with slow kinetics, release is delayed and the threat period is used to prepare and implement measures to protect the public (such as an evacuation).

At the end of the emergency phase, other protective actions are to be implemented or started in the contaminated areas to protect the population against the deposition of radioactive substances and to provide assistance to residents and others directly affected. These actions prepare for the post-accident phase during which the long-term consequences of accidental radioactive releases in the environment will be managed. According to the policies applied in the post-accident situations mentioned above, the following phases can be defined:

1. a **transition phase**, which starts at the end of the emergency phase. This phase varies in length, depending on the scope of the accident, and aims to limit the exposure of people and economic actors residing or working in the areas affected by the deposition of radioactive substances. It occurs in a context of rapid changes to the radiological, economic and social situations;
2. a **long-term phase**, which may last several years or decades, depending on the scope of the accident. Based on an accurate characterization of the radiological situation of the environment, including foodstuffs, this phase focuses on planning for the future of the affected areas so that they may return to conditions that are as normal as possible, as quickly as possible.

[996] There are also accidents where releases are immediate and sustained over time, as in the Chernobyl accident.

38.2. General organization of radiological emergency management

38.2.1. Organization and entities concerned

In the event of an accident (emergency situation) affecting a nuclear facility such as a nuclear power reactor, specific organizational measures are taken to implement the actions mentioned in the previous section. In the case of a nuclear power reactor, these measures concern the operator, the prefect of the *département*, and ASN and its support organizations (the public health agency *Santé publique France*[997], the weather service Météo France and IRSN, to name a few).

The roles and responsibilities of the various entities involved in an emergency are defined in an interministerial directive dated 7 April 2005[998] (currently being revised).

In a radiological emergency situation, as in a normal operating situation, the operator is responsible for the nuclear safety of its facility. At the facility level, the facility manager or his/her representative takes the actions necessary according to the on-site emergency plan[999] (see Section 17.9) to protect people at the site and any responders, to apply the procedures for limiting radioactive releases and restoring a controlled, stable state in the facility, to alert ASN and the prefect of the relevant *département*, and to inform the media.

Alerted by the operator, the prefect of the *département* may decide to activate the off-site emergency plan (covered in Section 17.7). The roles and responsibilities of prefecture authorities and mayors are described below in Section 38.4.

In compliance with the French Public Health Code (Article R.1333-83[1000]), before deciding to take measures to protect the population and reduce radiological exposure as much as reasonably achievable, the prefect of the *département* considers not only the support, information, and recommendations provided, but also the potential adverse effects associated with the measures planned compared to the expected benefits.

Nationally, ASN has several roles and responsibilities in emergency situations involving management of the situation, support (recommendations) provided to the

[997] The national public health agency (*Santé publique France*) is a French state-owned administrative entity under the supervision of the minister in charge of public health. *Santé publique France* replaced the National Health Surveillance Institute (*Institut de veille sanitaire*, InVS), the National Institute for Prevention and Education in Health Affairs (*Institut national de prévention et d'éducation pour la santé*, INPES), and the Organization for Public Health Emergency Preparedness and Response (*Établissement de préparation et de réponse aux urgences sanitaires*, EPRUS).

[998] Interministerial directive of 7 April 2005, relating to action by public authorities in response to an event involving a radiological emergency (JORF No. 84 of 10 April 2005).

[999] A specific on-site emergency plan is established for each nuclear power plant.

[1000] Excerpt not modified by later amending decrees (Decree No. 2007-1582 of 7 November 2007 and Decree No. 2018-434 of 4 June 2018).

national government, and communication. These roles and responsibilities are detailed in Section 38.5.

To perform its roles and responsibilities, ASN relies on IRSN's technical analysis of the situation, which is compared with the operator's view. This analysis includes both a diagnosis and a prognosis of the situation, covering the state of the affected facility as well as the environmental impact.

IRSN provides its technical expertise to public authorities and proposes both technical and public health or medical measures to protect the population and the environment and to restore a controlled, stable state in the facility. Protection measures mainly involve the distribution of stable iodine, sheltering within homes, evacuation in the most severe cases, restricting the consumption of foodstuffs and prohibiting their sale. IRSN cooperates with the French weather service, Météo France, which provides meteorological data used to calculate simulations of the transport and dispersion of releases of radioactive substances in the environment.

Depending on the severity of the radiological emergency situation and its progression, the national government's response may lead to the activation of the Interministerial Emergency Response Group (*Cellule interministérielle de crise*, CIC)[1001] in addition to action taken by the prefects of the *département* and the zone. As the instrument used for operational management of the emergency, the CIC, operating under the responsibility of the Prime Minister[1002], brings together all the relevant ministries, ASN, and, as necessary, the operator's representatives. The CIC takes charge of:

- centralizing and analysing all information related to the current radiological emergency,
- defining scenarios predicting the possible progression of the situation,

[1001] Generally managed by the French Ministry of the Interior, located in Paris. A 'limited' emergency, managed locally by the prefect (or the prefect of the defence and security zone) and the mayor(s) concerned, becomes a 'major' emergency based on its scope, media coverage, impact on multiple business sectors and its international dimension.

[1002] During a nuclear or radiological emergency, the State adopts organizational measures based on those defined in the interministerial circular No. 5567/SG of 2 January 2012, relating to government management arrangements for major emergencies. At the national level, the Prime Minister, in cooperation with the President of the French Republic, leads the government's political and strategic action to manage major emergencies requiring a coordinated response of public authorities. The Prime Minister prepares and coordinates government action to be taken in the event of a major emergency; if an actual major emergency occurs, he or she appoints the minister who acts on his or her behalf to head operational coordination of the emergency. The Prime Minister also relies on the Interministerial Emergency Response Group (CIC). The Prime Minister receives support from the General Secretariat for Defence and National Security (SGDSN, see also Footnote 1004) to coordinate the preparation and implementation of defence and national security measures incumbent upon various ministerial departments and to ensure the coordination of civil and military resources to be provided in the case of a major emergency. In a radiological emergency requiring a coordinated response from the State, SGDSN proposes appropriate strategies to the Prime Minister for managing the emergency and bringing the situation under control.

- preparing government decisions and coordinating their implementation between ministries,
- preparing information for the public and the government's communication approach.

A national alert system to mobilize the people concerned is a prerequisite for setting up all the resources required to respond to a radiological emergency. It is based on a system used to alert ASN and the prefect that can be activated directly by the affected nuclear power plant 24 h a day, 7 days a week. Once alerted, ASN and the prefect respectively alert the assessment organizations and the local and national government authorities. With this alert system, IRSN is able to mobilize its response organization within one hour.

Finally, as part of international conventions, for a radiological emergency in France, ASN notifies stakeholders of the event and provides information to international organizations (IAEA and the European Union[1003]) and to bordering countries that may be affected by the consequences of the situation. ASN also receives alerts and information from the IAEA and third-party countries if an event occurs outside of France.

38.2.2. Major Nuclear or Radiological Accident National Response Plan and emergency plans

38.2.2.1. Major Nuclear or Radiological Accident National Response Plan

The Major Nuclear or Radiological Accident National Response Plan[1004], released in February 2014, describes the organization of emergency response at the national level, the strategy to be applied (Part 1: Response Strategy and Principles), and the main measures that the national government may take to manage this type of accident (Part 2: Decision-Making Guide). It specifies how emergency response is organized at the national government level and reviews the roles of the relevant ministers, safety regulators, assessment organizations, and the operator in question. It covers both the actual emergency phase and preparation of the post-accident phase.

[1003] ECURIE (European Community Urgent Radiological Information Exchange).

[1004] No. 200/SGDSN/PSE/PSN – February 2014 edition. As a service within the executive branch of government, the General Secretariat for Defence and National Security (SGDSN) operates under the responsibility of the Prime Minister. SGDSN has three roles. The first involves providing surveillance and alerting authorities of any threats or risks. SGDSN is thus in charge of overseeing emergency situations, preparing government plans (such as the Major Nuclear or Radiological Accident National Response Plan), and organizing State authorities in the case of an actual emergency. Its second role is to make recommendations and draft decisions taken by executive authorities in the area of defence and national security. Finally, it acts as an operator, especially in managing security clearances, classified documents, government communication, the security of information systems, and cyber defence.

The plan covers various areas of emergency response management:

- national governance and its relationship with the local level (prefects and mayors),
- assessing and anticipating the situation,
- protecting the population against exposure to radioactivity,
- informing the public and coordinating communication,
- managing flows of people and maintaining order,
- providing medical treatment to victims and any people exposed to radioactivity,
- ensuring continuity of economic and social activities and initiatives taken by citizens for their own safety and that of their families and neighbours,
- coordinating relations at the European and international levels,
- early implementation of arrangements necessary for post-accident management, resuming societal functioning and economic and social activities (the principles and actions of post-accident management are included in the policy established by CODIRPA).

This response plan is based on reference situations rather than specific accident scenarios, as it is obvious that the progression of an actual accident cannot be defined in advance. It is a flexible plan that can be adapted to changes in a specific situation. Eight reference situations were adopted, of which three (identified as 1, 2, and 3) may involve an accident specifically affecting a nuclear power reactor:

- Situation 1: an established, immediate, short-duration release (lasting a few hours); the consequences are in theory moderate and may concern zones measuring up to a few kilometres (off-site emergency planning zones);
- Situation 2: an established, immediate, long-duration release (lasting a few days to a few weeks); the consequences may be much more significant and involve extended distances;
- Situation 3: a threat of release that may or may not be followed by a delayed release (a few hours after the accident starts) that lasts a long time (a few days to a few weeks); the consequences may also concern extended distances.

The other situations described in the national response plan cover 'uncertain situations' (release suspected, accident not yet characterized, etc.), transport accidents, accidents in other countries and accidents at sea.

38.2.2.2. Emergency plans

In a radiological emergency, two authorities are in charge of setting up concrete arrangements at the local level: the operator and the prefect. Each of them implements an emergency plan:

- The **on-site emergency plan**[1005] prepared by the operator (already covered in Section 17.9) indicates the specific organizational arrangements and the resources planned to manage significant events. It aims to protect and provide assistance to all people at the site, preserve or restore facility safety, and mitigate consequences affecting the public and the environment. It also specifies the arrangements made to ensure information is provided to public authorities and the media. In the case of reactors in the nuclear power plant fleet, two other types of plan have been established:
  - a mobilization and support plan for managing certain situations that require specific organizational measures[1006],
  - a security protection plan, if a malicious act is involved.
- The operator is responsible for activating and implementing the on-site emergency plan.
- The **off-site emergency plan** implemented by public authorities, prepared by the prefect and deployed under his or her authority, aims to protect the public, property, and the environment from specific risks (in the present case, radiological risk) related to the existence of a structure or facility. It reflects the civil security policy in terms of mobilizing resources, providing information and alerting. The off-site emergency response plan is a specific arrangement within the ORSEC plan mentioned above. The prefect of the *département* in which the accident occurs is responsible for activating the off-site emergency response plan. In the case of a large-scale event, measures to be taken beyond the boundary of the off-site emergency plan, including by the prefects of other *départements* potentially affected, are part of the Major Nuclear or Radiological Accident National Response Plan.

The specific off-site emergency response plan applicable to reactors in the nuclear power plant fleet includes three possible types of action:

- a 'first responder' phase that involves sheltering the population and listening for instructions within a 2-km radius around the facility; it is activated when immediate accidental release has occurred;
- an immediate phase of evacuating the population within a 5-km radius when long-duration release is anticipated in the short term (a few hours);
- a concerted-action phase during which the prefect may need to consider ASN recommendations and initiate (or change) other protective actions over distances based on the assessment of the situation. These distances may be

[1005] There are several on-site emergency plans for each NPP: 'radiological safety', 'nuclear safety with regard to weather- and climate-related events', 'toxic substances', 'fire outside controlled areas' and 'victim assistance' (see Section 17.9).

[1006] For example, mobilization for technical assistance, victim assistance and nuclear material transport.

shorter or longer than the radius covered by the off-site emergency response plan (for food consumption, for example).

The off-site emergency plan also provides for building preparedness within the population with regard to nuclear and radiological risk and a precautionary distribution of stable iodine within a 20-km radius around the facility.

38.2.2.3. Provisions for protecting the public in the event of an accidental release of radioactivity

Provisions for protecting the public in the event of a radioactive threat or release aim to limit the exposure of people to radioactivity, keeping it to a level as low as reasonably achievable. According to French regulations (Public Health Code), the measures to be taken in an emergency phase take into account:

- a reference level for the effective dose set to 100 mSv. While this is not a strict limit, it is considered inappropriate to exceed this level of exposure. ICRP notes that "a dose of about 100 mSv almost always justifies protective action". It adds that exposure above 100 mSv would only be acceptable in extreme situations, either because exposure is inevitable, or to save a life, for example, or prevent the situation from becoming worse;
- dose 'guidance values' to activate protective actions (sheltering, evacuation, iodine thyroid blocking) when exposure of the population may exceed these values[1007]. But it is important to note that public authorities may decide to implement these protective actions at different dose levels that are lower or even higher, depending on analysis of the advantages and disadvantages in the specific context of the actual accident situation[1008]. In this regard, local issues and the predicted kinetics and diffusion time of the release, more than its assessment which includes inaccuracy and conservatism, are pertinent criteria for guiding action to protect the population in a real-life situation.

Restrictions on the consumption of foodstuffs liable to be contaminated are also applied.

[1007] These guidance values are:
- effective dose of 10 mSv (for this concept, see Section 1.1.2 of this book) for sheltering and listening for instructions; the people concerned are alerted (by a siren or other procedure), they take shelter inside a building with all openings carefully closed (but not sealed), and they listen to the radio for instructions from the prefect;
- effective dose of 50 mSv for evacuation; the people concerned are instructed to pack a bag, close and lock their house, and leave (in an orderly fashion);
- equivalent dose to the thyroid of 50 mSv (see Section 1.1.2), for stable iodine administration (in the form of potassium iodide tablets and according to an age-specific dosage), in the case of release containing radioactive iodine (which may be the case for accidents affecting a nuclear reactor).

[1008] The French Public Health Code does allow the prefect flexibility in decision-making (Article R.1333-86).

Sheltering[1009] is a provision that, in theory, is easy to apply in the short term and will initially be given priority for accidents with fast kinetics. The goal is to reduce the public's exposure to external irradiation through the protection afforded by building structures, and to exposure through inhalation by reducing radioactive contamination of the air inside buildings. For an improvised shelter, exposure time is limited (to less than about 12 h) by the capacity of people to withstand the sheltering conditions. Sheltering may last several days if it is prepared in advance. But the efficiency of this protection decreases over time due to the gradual dispersion of radioactive substances inside buildings (through cracks, door and window frames, etc.).

Evacuation covers both the evacuation of independent people using their own means and assistance provided by public authorities to evacuate dependent people. The location of the evacuation centre for these evacuees must be chosen so that further evacuation will not be necessary due to changes in local weather conditions during accidental release.

Administering stable iodine is only useful if the release contains radioactive iodine (which may be the case for an accident involving a nuclear reactor). The purpose is to saturate the thyroid gland at an early stage to limit its absorption of radioactive iodine, which would increase the risk of cancer in this organ. This measure is most effective when stable iodine is administered at the required dosage about two hours before exposure to any release. It then gradually decreases, but a second administration may be considered. The decision to administer stable iodine is broadcast by approved media outlets with an indication of the dosage, the time of administration, and those to be given priority (children and pregnant women in particular). Implementing this decision is based on two types of distribution:

- preventive distribution of potassium iodide tablets around the facilities presenting a risk of exposure to released radioactive iodine,
- distribution to all points in the country during an emergency, using stocks kept by the corresponding *département* or zone (ORSEC iodine plan).

The prefect decides whether or not to apply restrictions on food consumption or performing certain activities (such as outdoor sports) depending on the situation.

38.3. Management by the operator

Information is presented below describing how the operator, EDF, manages an emergency situation (more specifically, when the on-site emergency plan involving radiological safety is activated). This discussion covers other aspects of emergency preparedness in addition to those mentioned in Chapter 17 on core-melt accidents[1010].

[1009] Being in a shelter does not exclude going out occasionally.

[1010] But it must once again be noted that an on-site emergency plan can be activated for emergency situations that do not necessarily imply the severity of a core-melt accident, etc.

▶ General organization

In an emergency situation, the response organization replaces normal operating conditions to alert and mobilize resources in order to bring the situation under control and mitigate the consequences, to protect personnel and provide them with assistance and information, and finally, to inform public authorities and implement a communication strategy.

EDF mobilizes its teams at two levels: nationally with a dedicated National Emergency Command Centre and National Emergency Response Team, and locally at the relevant site (or nuclear power plant). Organization at the local level is discussed below.

For each site, the planned organizational arrangements are described in a specific document kept up to date (the On-site Emergency Plan Site File), indicating the distribution and roles of the various teams and their interaction. The plan describes actions assigned to certain team members in greater detail.

▶ Emergency response teams at the local (site) level

Local-level emergency operating organization at EDF[1011] is based on:

– a decision-making centre, or the Site Emergency Command Centre;

– four operational centres:

  - the Facility Local Command Centre, in the control room,
  - the Site Radiological Command Centre,
  - the Site Logistical Command Centre,
  - the recently organized Nuclear Rapid Response Force (FARN) Command Centre (see Section 36.6.6), created subsequent to operating experience feedback from the Fukushima Daiichi nuclear power plant accident.

The Local Command Centre, where operational actions are based, consists of members of the shift personnel, working under the authority of the shift manager. The Local Command Centre is therefore installed in the reactor control room or, if this room must be evacuated (for example, in the case of fire), in the remote shutdown station. The shift manager raises the alert across the site and contacts potential backup personnel at home. In the control room, the shift manager supervises and monitors operations performed to control and protect the facility. If specific and predetermined criteria are reached, the shift manager calls the member of the Site Emergency Command Centre acting as the Emergency Response Director and requests activation of the on-site emergency plan. Outside business hours, if the emergency response director cannot be reached, the shift manager activates the on-site

[1011] Unless otherwise indicated, the various teams described gather in rooms dedicated specifically to managing emergency situations.

emergency response plan and, if necessary, the first-responder phase of the off-site emergency plan.

The Site Emergency Command Centre contacts the EDF National Emergency Command Centre, ASN, and the prefect of the *département*. For an assessment of the situation, it turns to the Local Emergency Response Team. Support from a physician is also provided at the Site Emergency Command Centre.

The Local Emergency Response Team is mobilized in what is called the Technical Support Centre. The Local Emergency Response Team is in charge of analysing the situation and its predictable progression (according to the '3D/3P' method, described below), proposing actions it considers necessary to the Site Emergency Command Centre, and sending its analysis of the situation to the Site Radiological Command Centre. The Local Emergency Response Team is in contact with the National Emergency Response Team and IRSN (Emergency Response Centre – see below).

The Site Radiological Command Centre is both an operational and a support centre. It maintains contact with the National Emergency Response Team and IRSN to exchange information and cooperate on issues involving release, radiological consequences, measurements in the environment and forecasts. The Site Radiological Command Centre is divided into two units: a Computing Unit in charge of forecasts and a Monitoring Unit in charge of taking measurements in the environment and processing this data.

The Site Logistical Command Centre is an operational centre in charge of support actions for logistics (vehicles and transport, marking and signalling, equipment supply), telecommunications, maintenance, protection of people, security, and radiation protection. It is responsible for activating the remote shutdown station. It is only in contact with the site's internal entities (Site Emergency Command Centre, Facility Local Command Centre and Site Radiological Command Centre).

The Nuclear Rapid Response Force (FARN) Command Centre is only activated if the decision is made at corporate level to deploy this force (decision made by the National Emergency Command Centre).

38.4. Prefectural authorities and mayors

In a radiological emergency, the prefect of the *département* in which the event originates is responsible for overseeing all emergency response operations, except inside military areas. This includes operations involving policing, security, and public health. The prefect receives support from ASN and IRSN.

In an emergency response situation, the roles and responsibilities of the prefect are as follows:

– alerted by the operator, the prefect immediately alerts the appropriate organizations and authorities;

- the prefect defines the perimeter within which the population and elected officials are informed of the radiological emergency, the appropriate behaviour to adopt, and the applicable public health actions; the prefect changes this perimeter depending on how the situation progresses;
- the prefect decides whether or not to activate the off-site emergency plan and sends preparatory instructions to organizations with specific collective responsibilities. For this purpose, the prefect continuously monitors actions taken by the various assistance, response and protection teams to ensure that they are consistent with one another;
- the prefect implements any bilateral agreement(s) with the appropriate counterparts in countries that border the *département*;
- the prefect prepares and initiates as needed the response actions for long-duration exposure situations resulting from a radiological emergency.

When the needs for protection of the population and the environment extend beyond the scope of the off-site emergency plan, the prefect implements the ORSEC Plan[1012].

The prefect also provides information to the population and the media.

The prefect is supported in this action by the mayors of the cities involved, who in turn rely on arrangements defined in their Community Safety Plan.

If an accident affects several *départements*, a prefect is assigned to this Defence and Security Zone, who is responsible for executing national security measures within this zone. This person is in charge of coordinating:

- measures taken by the various prefects whose *département* is affected by the consequences of the accident,
- local communication of the prefects, in coordination with information released by the national government,
- backup and support necessary in order for prefects to take action.

38.5. ASN, the Nuclear Safety Authority

In compliance with the French Environment Code (Article L.592.32), ASN is associated with the management of radiological emergencies resulting from events occurring in France or liable to affect French territory that could have adverse effects on human health and the environment due to exposure to ionizing radiation. For this purpose, it participates in the Interministerial Emergency Response Group (CIC), if it has been activated.

[1012] Civil security emergency response plan (*Organisation de la réponse de la sécurité civile*).

ASN collaborates as necessary with public authorities to ensure preparedness for radiological emergencies. In particular, it provides technical assistance to the competent authorities for developing arrangements within emergency response plans that take into account risks resulting from operations conducted by facilities included in the scope of its expertise. It also ensures that nuclear operators and those in charge of civil nuclear activities comply with their obligations in terms of developing their emergency plan.

In a radiological emergency, ASN:

- alerts its support organizations (*Santé publique France*, Météo France, IRSN, etc.) so that they can provide the necessary technical support,
- ensures that the measures taken by the operator to mitigate the consequences of the accident are valid and oversees their implementation,
- makes recommendations to the government and its local representatives (prefects representing a *département* or a Defence and Security Zone) on measures to be taken to protect the population, property and the environment,
- participates in providing the public with information on a nationwide basis.

ASN helps the State fulfil its obligations under international conventions[1013].

For nuclear facilities and activities within its scope, it is the competent national authority in application of the international Convention on Early Notification of a Nuclear Accident dated 26 September 1986 (in force in France since 6 April 1989) and the European Council decision of 14 December 1987 concerning European methods for rapid exchange of information in the event of a radiological emergency.

ASN is also the competent national authority in application of the international Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, signed by France on 26 September 1986.

38.6. IRSN

Decree No. 2016-283 of 10 March 2016 relating to the French Institute for Radiological Protection and Nuclear Safety, Article R.592-1, stipulates that IRSN "proposes technical, health, and medical measures to ASN in the event of an incident or accident involving sources of ionizing radiation. These measures are taken to ensure protection of the public, workers[1014] and the environment and to restore security in the facilities. In these circumstances, IRSN also provides technical support as needed to other

[1013] An interministerial directive of 30 May 2005 concerns the application of the international Convention on Early Notification of a Nuclear Accident and the decision of the European Council concerning European methods for rapid exchange of information in the case of a radiological emergency. An interministerial directive of 30 November 2005 concerns the application of the international Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency.

[1014] Including emergency response teams.

State authorities concerned." According to the Major Nuclear or Radiological Accident National Response Plan mentioned above, IRSN is one of the actors called upon in an emergency to provide support to safety regulators and ministries.

For this purpose, IRSN draws on its knowledge of facilities and their associated risks, on the results of calculations performed using specific simulation tools, and on the results of contamination measurements taken in the environment or contamination monitoring performed on people, either near the site of the accident or in permanently installed IRSN laboratories. It participates actively in taking these measurements by sending out its mobile units or by mobilizing its permanent laboratories. In addition, IRSN also takes part in providing information to the public.

More specifically, when an emergency occurs, IRSN assesses the risks related to the situation and its actual or potential radiological consequences in order to propose protective actions that can be implemented by public authorities. This assessment includes both a diagnosis of the situation and a prognosis of its possible progression. The diagnosis involves the state of the affected facility, whether or not radioactive substances were released, their dispersion in the environment, and the consequences in terms of exposure of the population (including workers) and the environment (foodstuffs, livestock, etc.) to ionizing radiation. The purpose of prognosis is to determine the possible consequences and provide early recommendations on the appropriate protective measures. The assessments performed by IRSN in emergency situations affecting a nuclear facility are discussed with the facility operator and are compared with the operator's own assessments.

IRSN experts may be assigned to work with public authorities, for example, with the Interministerial Emergency Response Group or the prefect of the concerned *département*, as well as in ministerial operational centres, if the need has been expressed.

To fulfil its obligations in an emergency situation, IRSN has a specific response organization, based on the teams and tools belonging to the Emergency Response Centre, created in 1982 at the request of the SCSIN. IRSN also relies on mobile resources for measuring environmental and human contamination. The Emergency Response Centre consists of several units, each of which has its own roles and responsibilities, such as:

- assessing the state of the facility,
- assessing the radiological impact of the accident,
- deploying mobile resources for measuring contamination in the environment[1015],
- handling questions concerning the safety of workers and members of the public who might be affected,
- handling communication to meet the needs of the public, media and stakeholders.

[1015] The 'mobile unit' works with the local team mobilized by the prefect, in particular at the Operational Command Centre, if one has been set up, under the command of the Rescue Operations Commander.

IRSN has access to the following data at the Emergency Response Centre:

- a large amount of information on the affected reactor (state of equipment, data from the facility's instrumentation), received minute by minute via a computer link (through a system called the KIT/KPS, set up in 1988 – see Figure 38.1). Some of this information is provided in messages sent by the operator every 15 min ('15-min messages'),
- the results of measurements taken in the field, gathered by the mobile unit and centralized in a database called CRITER,
- the results of measurements taken using the Téléray remote monitoring network deployed by IRSN throughout France (ambient dose rates), – see the Focus feature below –,
- meteorological data sent by Météo France via a dedicated link, necessary for assessing the radiological consequences,
- human internal contamination measured using IRSN's mobile resources or monitored in permanently installed laboratories, then centralized in a tool called CRIHOM.

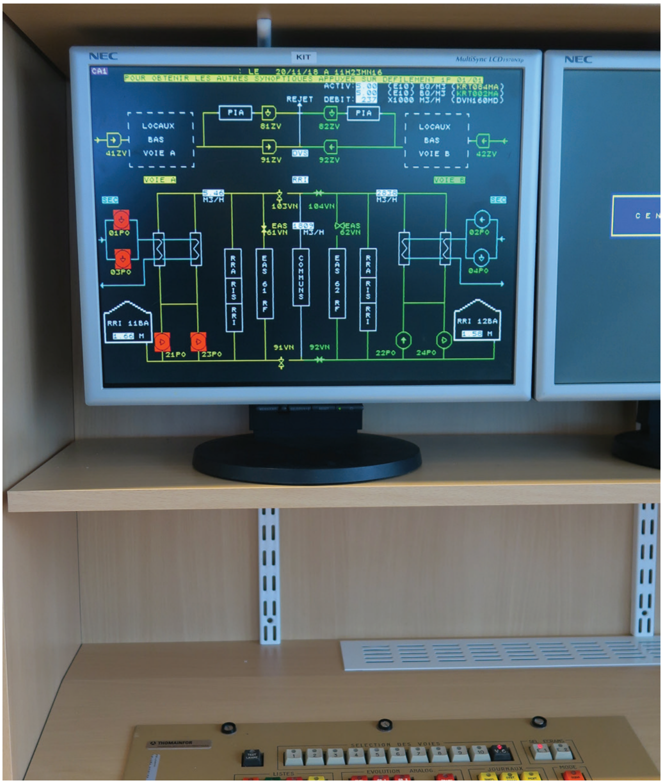


Figure 38.1. Partial view of the KIT/KPS. Stéphanie Clavelle/IRSN Media Library.

Calculation resources for assessing the state of the facility and releases are combined in a tool (or system) called SESAME (accident situation progression plan and assessment methods), operational since 1994. It has a set of calculation modules that, depending on the type of event (loss-of-coolant accident, steam generator tube rupture(s), etc.) and the reactor situation, can be used to estimate information such as:

- the size of the reactor coolant system break,
- time to core uncovery, cladding rupture and core melting,
- percentage of cladding rupture or core melt,
- hydrogen risk,
- radioactivity released and the associated kinetics.

The calculation resources for assessing the radiological impact are combined in the simulation system (or platform) called C3X. Based on available information on releases that have occurred or may occur, on the results of measurements in the field, and on meteorological data sent by Météo France, the C3X system can assess:

- short-range (up to 50-80 km) and long-range (above 100-120 km) atmospheric dispersion of released radioactive substances,
- soil deposits associated with this dispersion,
- exposure of people to ionizing radiation associated with this dispersion and these deposits, taking into account all potential exposure pathways (external irradiation by immersion in the radioactive plume or by deposits, internal contamination by inhalation of these substances or by ingesting contaminated foodstuffs, etc.).

The C3X system can also be used to create maps of the results of the assessments mentioned above.

The mobile unit has specific equipment (vehicles, radioactivity detectors, etc.) for performing its own measurements in the field and analysing samples taken in the environment. It also has resources for measuring human contamination[1016]. When mobilized, these resources are part of the Victim Reception Centre, a local structure set up by the prefect. Measurement results are sent to the unit in charge of healthcare questions. These Mobile Human Radiation Protection Units include four light-duty vehicles and two mobile laboratories for whole-body radiation dosimetry, as well as four heavy-duty vehicles for examinations of the thyroid and thorax.

[1016] In addition, at its Vésinet location, IRSN has a medical biology laboratory that performs radiotoxicology examinations of contractor personnel. The laboratory also handles human samples in the case of a nuclear or radiological emergency, to screen people for contamination.

#FOCUS

Téléray network

Created in 1991 after the Chernobyl accident, the Téléray network consists of a set of more than 400 probes (see Figure 38.2) spread throughout metropolitan France and in the French overseas *départements* and territories. It can rapidly detect an unusual increase in ambient radioactivity near these radiation monitors. The monitors are located as follows:

– about 100 probes provide overall monitoring in France (one monitor per *département*). They provide relevant data on air contamination in the event of a large-scale accident;

– about 300 probes monitor urban areas located between 10 and 30 km from nuclear facilities. These probes are a supplement to the operator's equipment, which covers a radius of 10 km around each site.

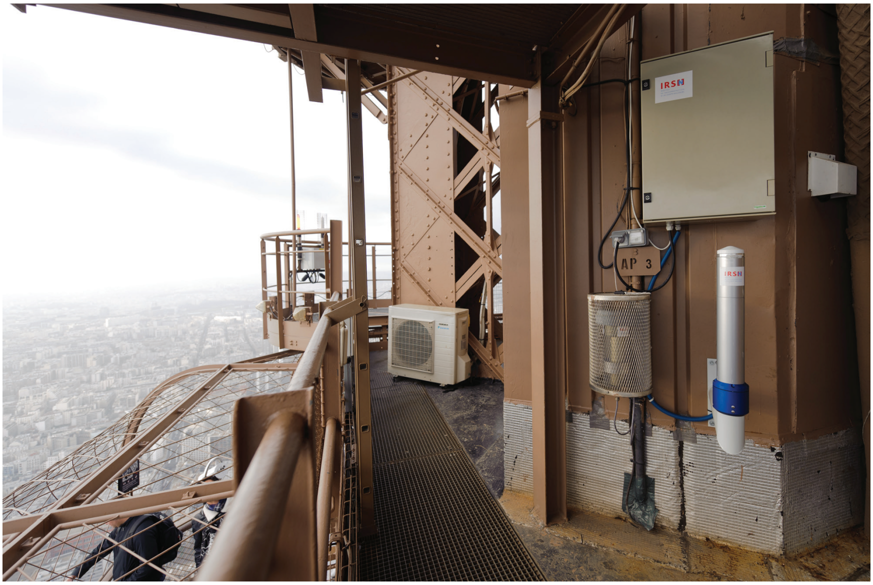


Figure 38.2. Téléray probe installed on the Eiffel Tower in Paris. Arnaud Bouissou/MEDDE/IRSN Media Library.

The Téléray probes, sensitive to gamma radiation, measure the ambient gamma dose rate, expressed in nanosieverts per hour (nSv/h). Their measurement range extends from 10 nSv/h to 10 Sv/h.

As soon as a measurement exceeds a threshold value (150 nSv/h above the usual measurements), an alarm is triggered at the remote monitoring centre, where the measurement is analysed to identify the source of the alarm: accidental release, radioactive source passing close to the monitor, natural phenomenon (radon) or malfunction.

If an accidental release is possible, the information is passed on to the IRSN duty engineer, who alerts the IRSN director general and the competent public authorities. Gamma dose rate measurements are available the day after their acquisition on an Internet site dedicated to the Téléray network[1017].

38.7. Assessment approach in the event of an accident affecting a reactor in the nuclear power plant fleet

The goal of the assessment approach is to evaluate the situation and its possible progression over time to make any recommendations needed in a timely manner regarding the actions required to protect people and the environment. Implemented cyclically, this approach is organized around the following actions:

- a diagnosis of the situation covering both the state of the affected facility, past and ongoing release of radioactive substances, and their radiological consequences in the environment. This diagnosis is based on analysis of technical data provided automatically or via messages sent by the operator of the affected facility, information on the actions conducted by the operator, assessment of radionuclide transfers to the environment and the results of available radiological measurements;
- a prognosis of how the situation will develop over time. Based on the diagnosis and measures taken in the facility, this prognosis serves to predictively assess changes in the state of the facility (in particular, the condition of the various confinement barriers for radioactive substances), future releases (quantities and time before release) and their radiological and dosimetric consequences;
- if necessary, a prognosis incorporating an aggravating event, i.e. assuming an additional equipment failure, to assess the impact in terms of release (quantities and especially time before release) and the radiological and dosimetric consequences in the environment;
- at regular intervals, comparison and discussion of the diagnosis and prognosis results relative to the operator's results;
- sending the results of IRSN's assessment and its proposed protective measures to be implemented or planned to ASN and possibly to public authorities.

[1017] National environmental radioactivity measurement network: https://www.mesure-radioactivite.fr.

Regular implementation of this assessment approach serves to adjust the diagnosis and prognosis of the state of the affected facility and any radioactive release (plumes, deposits, etc.), taking into account any changes in the affected facility's situation, meteorological updates sent by Météo France and contamination measured in the environment. The simulation tools used by IRSN estimate the corresponding exposure of people. Calculations are generally performed to obtain dose estimates that are reasonably bounding.

The discussion that follows refers mainly to an accident affecting a pressurized water reactor in a nuclear power plant. In principle, it applies to all types of reactors.

To successfully conduct the required assessments in an emergency situation, IRSN applies the methods and uses the simulation software described below. These assessments are regularly compared with those performed by EDF such that, if possible, there are no occurrences of criticality that are not understood during an emergency.

38.7.1. '3D/3P' method

The '3D/3P' method (triple diagnosis/triple prognosis) is a component of the assessment approach applied when a nuclear power reactor is affected by an emergency situation. The guiding principle behind this method was established by IPSN in 1983, in collaboration with EDF and Framatome. EDF then developed the method so that it could be applied in the event of an emergency at any one of its nuclear power plants. The method aims to structure the analyses conducted by the various emergency response teams and facilitate exchanges between them. It provides a regular assessment of the state of the facility and any changes it may undergo.

In this manner, in an emergency, the 3D/3P method can be used by EDF (more specifically by the Local Emergency Response Team of the affected nuclear power plant) as well as by IRSN, thereby establishing a common basis for sharing information.

The 3D/3P method involves periodic assessment of the state of the three physical confinement barriers (which explains the number '3' for a nuclear power reactor) that normally exist between the radioactive substances in the reactor core and the environment, as well as any possible changes they may undergo. The goal is to identify and characterize any actual or potential release of radioactive substances to the environment. The confinement barriers for a pressurized water reactor are presented in Chapter 7.

For each confinement barrier, the following actions are performed:

- a diagnostic analysis covering:
  - assessment of the state of the barrier,
  - assessment of the safety functions required to ensure the barrier's efficiency,
  - identification of the available systems that contribute to the safety functions;

- prognostic analysis covering:
  - a study on how system availability, thus the relevant safety functions, may evolve in time,
  - the corresponding assessment of how the state of the confinement barrier may evolve in time.

The triple diagnosis-triple prognosis method takes into account the state of the following components for the various reactor confinement barriers:

- for the first barrier, the state of cladding (whether it is leaktight) and the state of fuel (whether it has melted);
- for the second barrier, the state of the reactor coolant system (whether it is intact, questionable, or has a confirmed break). If there is a break in the reactor coolant system, it is necessary to determine whether the break is inside or outside the containment, whether there is an opening in one or more pressurizer relief lines, whether there is a break at the seals of the reactor coolant pumps, or whether there is a rupture of one or several steam generator tubes;
- for the third barrier, the state of containment integrity (normal leaks, direct abnormal leaks, abnormal leaks to the auxiliary buildings, use of filtered venting).

The reactor safety functions, relevant to each of the confinement barriers, are as follows:

- for the first barrier, controlling reactivity and maintaining the water inventory in the reactor coolant system,
- for the second barrier when the reactor coolant system is closed, heat removal from the reactor coolant system and heat removal from the seals of the reactor coolant pumps,
- for the second barrier when the reactor coolant system is open, heat removal from the reactor coolant system,
- for the third barrier, removal of heat released in the containment and containment integrity (effectiveness of isolation systems and depressurization and filtration of release by the annulus in 1300 MWe and 1450 MWe reactors).

The results obtained using this method are noted in a '3D/3P grid' that summarizes conditions clearly.

Following the prognosis, and if the start time of the actual or potential radioactive release is known, it is possible to predict the radiological consequences that could result and to recommend any actions required to protect the population.

38.7.2. The 'aggravated prognosis' approach

Operating experience feedback from emergency response exercises has shown that the prognosis made using the '3D/3P' method is not always sufficient to make timely decisions about certain protective actions. Prognosis is based on the state of the systems in the facility at the considered time and assumes that no new failures will occur, except those that are predictable based on the state of the facility (for example, loss of a water injection system in service once its water tank has been completely drained).

An 'aggravated prognosis' approach was thus developed to extend analysis of the situation and identify any failures that could lead to very rapidly recommending additional actions to protect the population. This approach involves postulating the occurrence of an additional hypothetical failure, independent of the progression of the current accident. Its impact in terms of release of radioactive substances is then estimated. If this release may lead to significant radiological consequences in a time frame incompatible with taking appropriate protective actions, taking these actions preventively may be recommended.

More specifically, this approach is an investigation method used to identify equipment in the facility whose failure would lead either to core melting in a short time or, if the prognosis of core melt is confirmed, to an increase in the maximum distances to which the protective actions already decided upon should be extended.

The aggravated prognosis approach was adopted by IPSN in the 1990s and discussed with EDF. Since the end of the 2000s, it has been used concertedly during exercises by EDF and IRSN.

38.7.3. Extending the 3D/3P method to severe accidents (the 'D/P AG' method)

The '3D/3P' method described above is not suitable for analysing core-melt situations in a pressurized water reactor. In these situations, the role of the first two confinement barriers is significantly reduced, specific risks emerge[1018], and there is a decrease in usable instrumentation. The decision was thus made to adapt the method to these situations, using a 'D/P AG'[1019] approach, while maintaining as much as possible the formal procedure used by EDF and IRSN emergency teams.

The D/P AG approach still considers the three confinement barriers, but the first barrier is considered to be the fuel itself and not the cladding. Like the 3D/3P method, the D/P AG method involves periodically assessing the state of the barriers and their predictable changes to identify and characterize any actual or potential release of radioactive substances to the environment.

[1018] See Chapter 17 (steam explosion, direct heating of gases in the containment, etc.).

[1019] 'D/P AG' stands for *Diagnostic/Pronostic en Accident Grave* (diagnostics and prognostics in a severe accident situation).

The triple diagnosis-triple prognosis takes into account the state of the following components for the various confinement barriers:

- for the first barrier, the percentage of core melt, as an indicator of the release of radioactive substances,
- for the second barrier, the type of reactor coolant system break (inside or outside the containment, an opening in one or more pressurizer relief lines, a rupture in one or more steam generator tubes) and the physical state of the vessel (whether or not melt-through has occurred),
- for the third barrier, state of containment (normal leak, direct abnormal leak, abnormal leak to the auxiliary buildings, use of the 'U5' procedure, whether or not basemat melt-through has occurred).

The safety functions associated with each of the barriers are as follows:

- for the first barrier, controlling reactivity and maintaining the water inventory in the reactor coolant system,
- for the second barrier, heat removal from the reactor coolant system and the vessel lower head,
- for the second and third barriers, removing heat released by the corium, whether it is in the vessel or the containment,
- for the third barrier, maintaining the water inventory in the reactor pit and the reactor building, removing heat released in the containment, controlling the composition of the containment atmosphere (with regard to the hydrogen explosion risk), maintaining containment integrity (ensuring that the isolation systems and depressurization of the annulus for 1300 MWe and 1450 MWe reactors perform correctly, as well as filtration of the associated release) and maintaining water inventory in the steam generators.

38.8. Emergency preparedness

The purpose of emergency preparedness is to ensure that, within the entities involved, whether national, regional, local or international, appropriate resources and equipment are in place to provide an appropriate response to any nuclear or radiological emergency. Attaining this objective, which covers all possible emergency situations, assumes that the following have been defined and are operational for each entity:

- roles and responsibilities,
- the emergency response organization and the associated personnel,
- coordination of activities within the response organization,
- procedures associated with the response organization,
- tools and equipment necessary to fulfil roles and responsibilities,

- personnel training (in the response organization, procedures, tools, stress management, etc.),
- personnel training.

Preparedness consists in ensuring that each entity concerned contributes the appropriate resources to the national response organization so that this organization can respond in the most appropriate manner to the radiological emergency situation. The resources required are evaluated in terms of their nature and the time required to set them into operation. As a reminder, the objectives of the national response organization are to:

- regain control of the situation and mitigate the consequences,
- protect the population by avoiding deterministic effects and mitigating the risks of stochastic effects,
- provide first aid and treatment for people in need,
- keep the public informed,
- protect the environment to the extent possible,
- prepare the economic and social resilience of the impacted zone.

For this purpose, at IRSN, several hundreds of experts are specially trained for the various roles they may have to play in an emergency. This represents more than 6000 h of training per year. In addition, these experts regularly practice their skills in role-playing exercises or even in actual emergencies.

38.8.1. Emergency response exercises

Emergency response exercises (see Figure 38.3) are performed to test all or part of the arrangements planned to manage a radiological emergency. The general objectives of these exercises are to:

- ensure that people are familiar with the plans (on-site and off-site emergency plans, community safety plan), that they are operational, and that the procedures they call for, including the alert procedure, are effective,
- more generally, ensure that the planned organizational arrangements and procedures are effective,
- train people who may be mobilized on how to manage this type of situation,
- help inform the media and the public.

Two types of exercises involving the national response organization and the prefects are organized by the relevant ministries and ASN; they mainly differ by their objectives:

- national nuclear safety exercises aim to test participants' reactions and the decision-making processes based on a technical scenario affecting the nuclear safety of a facility, without actual civil security actions involving the local population;

- national civil security exercises aim to test arrangements included in the various plans to protect the public and property, including actual implementation of significant actions in the field involving the local population. These exercises generally include media pressure on the various entities that participate. They also test response operations both on and off the site and the interface mechanisms in place.

In addition, exercises can be specifically performed independently of the exercises mentioned above to test how actions are carried out and check coordination of people and response teams in the field. This gives teams the opportunity to practice using environmental contamination monitoring equipment, for example, including IRSN's equipment.

Local exercises are also organized by operators to test their own organizational arrangements. These exercises do not mobilize the entities of the national response organization, except for IRSN, which may carry out a counter-assessment of the operator's assessment.

IRSN therefore participates each year in a total of about twenty exercises. Through these exercises, the Institute is able to regularly test its alert system, the mobilization and operation of its response organization with, if necessary, the deployment of its mobile units and, depending on the exercise objectives, the dedicated communication unit, as well as its assessment tools.

Figure 38.3. An emergency response exercise involving the Gravelines nuclear power plant. Shown here is the Site Emergency Command Centre team. Gravelines NPP.

Certain exercises have an international component, especially when the concerned facility is close to a border. In addition to these exercises, others are organized by the IAEA, along with workshops in the field, also organized by the IAEA, and still other exercises organized by the OECD. ASN and IRSN participate in international exercises.

In 1986, the Chernobyl nuclear power plant accident showed that nuclear accidents can have international consequences and that international cooperation is important in terms of media communication, exchanging information, and the planned emergency response in the various countries involved.

The IAEA therefore regularly prepares and organizes exercises and classes to assess and improve its own response arrangements and resources in the event of a nuclear or radiological emergency, as well as those of its member countries. The exercises conducted to test the operational arrangements of the Convention on Early Notification of a Nuclear Accident and the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency are ‘convention exercises’, called ConvEx. They aim to assess and improve, as necessary, the international framework for emergency preparedness and response.

ConvEx exercises have different levels of complexity, ranging from a test of emergency communication lines with the ‘contact points’ in member countries (ConvEx-1 exercises) to large-scale exercises covering the early phase of a significant radiological emergency (ConvEx-3 exercises) which are organized once every three to five years, based on a national exercise in a member country. The ConvEx-3 exercises aim to assess and improve, as necessary, information exchange, mutual assistance and the coordination of information provided to the public.

The exercises organized by the OECD in the same areas are called International Nuclear Emergency Exercises (INEX).

Reports on the international exercises mentioned above have been made public.

38.8.2. Operating experience feedback

After each exercise, immediate debriefings are organized by the managers of the teams that participated in the exercise. They review the participants’ experience of the exercise, the difficulties encountered and other aspects. Lessons learned from these exercises are used to develop corrective action plans or plans to improve work methods, organizational arrangements or resources. For national exercises, an operating experience feedback meeting is also organized a few months after the exercise between the representatives of the entities involved (ASN, operator, prefect, IRSN, etc.).

Following an actual emergency, operating experience feedback is collected using the same approach. For example, the Fukushima Daiichi nuclear power plant accident, for which IRSN’s response organization was activated for six weeks, led to defining and implementing changes to this organization.

Part 5

PWR Safety Studies, R&D and Simulation Software

Chapter 39
PWR Safety Studies and R&D

This chapter is not intended to present all of the studies and R&D which, as part of development of the French nuclear power programme, were carried out by the designer[1020] (initially under licence from Westinghouse), Électricité de France (EDF) and CEA, whether it be to support reactor design or for the purposes of operation, periodic reviews[1021] or integration of feedback from accidents in other countries such as those in the nuclear power plants at Three Mile Island (1979), Chernobyl (1986) and Fukushima Daiichi (2011). Similarly, it is not possible here to provide an exhaustive presentation of the studies and R&D conducted by IPSN (established in 1976 within CEA) and later IRSN to perform their safety assessment missions, many of which are carried out in collaboration with the organizations mentioned above.

The purpose of this chapter is to provide a brief overview of the topics covered in studies and R&D for pressurized water reactor safety, as well as national and international R&D programmes, the main organizations involved, and finally some of the research facilities that exist in France. Research and development has made it possible to identify certain risks and improve knowledge, in particular concerning phenomena that can occur in accident situations. For a certain number of safety topics, studies and R&D have led to modifying equipment or installing new equipment in nuclear power plants, new operating procedures to better control certain accident situations or to deal with accident situations that were not considered when the reactors were designed, the use of new high-performance technologies and other aspects.

[1020] Framatome before 2006, then Areva (NP), and Framatome as of 2018.

[1021] These are the studies included in the reassessment part of periodic reviews, as defined in Section 30.3.

This chapter does not cover studies carried out by the designer and EDF in the reactor design stage; some examples for the EPR are given in Chapter 14 on probabilistic safety assessments and in Chapter 17 on the consideration of core-melt situations in the design of this reactor. Chapters 8, 11 and 12 outline approaches to design studies on operating conditions and hazards. The approach applied in these design studies ('design study baselines'), such as the initial reactor states considered, the state of the core (start of cycle, end of cycle, etc.), data sets, assumed aggravating events and technical acceptance criteria, is discussed with safety organizations at an early stage in the reactor project. Subsequently, these study methods may evolve in the context of periodic reviews of the reactor to take into account new knowledge from R&D (as illustrated in chapters 9 and 35 concerning respectively loss-of-coolant accidents and reactivity insertion in pressurized water reactors).

The next chapter is devoted to simulation software.

39.1. Contribution of studies to the improvement of pressurized water reactor safety

Once reactors have been commissioned, events that occur during operation often provide a reason to initiate studies to properly identify their causes, assess any potential risks if aggravating events were involved to learn as much as possible from them, and to better assess their severity in terms of safety. The studies carried out following the error that occurred in 2001 during core refuelling at Unit 4 of the Dampierre-en-Burly nuclear power plant, referred to in Section 35.3, are an example of this. 'Precursor' and 'Recuperare' type analyses, described in Chapter 21, also fall into this category of studies; the former use probabilistic safety assessment models.

Probabilistic safety assessments, carried out or updated in the context of the 10-yearly inspection programmes of the French nuclear power plant fleet, constitute a privileged general framework for systematic, in-depth analysis of these reactors, which has proved to be relevant for enhancing the level of safety.

Reactor equipment and organizational changes are sometimes made as the direct result of probabilistic assessments followed by (Level 1 and Level 2) probabilistic safety studies or physical and functional support studies, some of which are presented in Chapter 14; examples include:

- taking into account complementary situations, with installation of additional equipment and preparation of beyond-design-basis operating procedures (the 'H procedures');
- implementing measures to reduce the risk of core melt in reactor shutdown states when the reactor coolant system is partially drained, to the level of the hot and cold legs ('mid-loop operation' of the residual heat removal system);
- changing the containment sump filters; this change was carried out to address the risk of filter clogging in the core cooling mode where water is recirculated in the containment, resulting in improved reliability of this cooling mode;

- enhancing the equipment hatch closure system at the flanges that ensure the connection to the reactor building in order to keep the containment leaktight in the event of overpressure resulting from core melting;
- adding thickness to the basemats at the Fessenheim nuclear power plant to increase the time before basemat melt-through in the event of a corium leak from a molten core;
- installing instrumentation to detect vessel melt-through in the event of core melt, in order to address emergency situations.

Studies (associated with R&D) already initiated before the accident at the Three Mile Island nuclear power plant, and supported by data available subsequent to this accident, led to the installation of new equipment such as the containment filtered venting system (U5) and the autocatalytic hydrogen recombiners (see Chapter 17).

After the Chernobyl nuclear power plant accident, studies resulted in designing and implementing measures to avoid reactivity accidents caused by transfer of non-borated or cold water into the core (see Chapter 35).

In general, the accident that occurred in 2011 at the Fukushima Daiichi nuclear power plant has supported the case for R&D in areas such as core-melt accidents and external hazards (earthquake, flooding). In concrete terms, studies have led to implementing the 'hardened safety core' and EDF's Nuclear Rapid Response Force (FARN), discussed in detail in Chapter 36. The accident also gave rise to studies on emergency response management in extreme situations from the perspective of human and organizational factors. IRSN released two reports[1022] highlighting avenues for further study.

Studies are carried out taking into account the best knowledge available (on equipment reliability, complex physical phenomena, etc.) and using state-of-the-art simulation tools, thereby taking advantage of research and development findings achieved both in France and in other countries. Since EDF and IRSN conduct their studies independently for their own intents and purposes, EDF as the operator responsible for facility safety and IRSN as the outside expert in charge of assessments, the validity of the methods, assumptions and simulation software used by each entity needs to be clearly supported so that conclusions can be drawn through analysis of both views, allowing ASN to take operational decisions.

A general overview of research and development in pressurized water reactor nuclear safety is presented below, with examples of some of the most significant or ongoing work.

[1022] A Human and Organizational Factors Perspective on the Fukushima Nuclear Accident, IRSN report PSN-SRDS/SFOHREX 2015-01 (7 April 2015), and *Six questions pour tirer les leçons de la catastrophe de Fukushima sur le plan des facteurs organisationnels et humains* (Six Questions to Draw Conclusions from the Fukushima Disaster in Terms of Human and Organizational Factors), IRSN report NHP-RSDS/SFOHREX 2015-02 (7 April 2015).

39.2. Purpose and overview of R&D work, dedicated programmes and organizations involved, and research facilities in France

39.2.1. Purpose and overview of R&D

As in any other industry, research and development is necessary to achieve better performance through improved design and operation of nuclear facilities. It is also intended to advance facility safety with regard to issues raised in the context of safety analyses, emergency preparedness and response and in the aftermath of significant accidents.

Research and development in the field of pressurized water reactor safety has contributed to:

- improving knowledge of the phenomena at work in accident situations, which can sometimes be complex;
- developing and validating physical models and simulation software;
- exploring new technologies that could be used to enhance safety;
- better identifying human and organizational factors that can leverage improvements in operational safety or emergency management;

and, as stated in the previous section, providing substantiation for various safety studies – in particular those conducted for periodic reviews – by making available, for example, the most advanced, qualified and relevant simulation software, given acquired knowledge.

The results of R&D can serve, in particular, to evaluate or reassess, on sound physical principles – sometimes incorporated in simulation software – the conservatism of design options and choices made in the associated safety studies. As indicated above, in France, the safety reassessments associated with the 10-yearly inspections of nuclear power reactors can be the occasion, if necessary, to apply new knowledge resulting from this research work in an operational context.

R&D work in the area of pressurized water reactor safety is part of the general approach to preventing and mitigating postulated accident situations (including hazards) examined in several of the previous chapters. Certain research projects focused specifically on safety are briefly presented below[1023], with some of the more important phases.

[1023] For further details, see Jean Couturier and Michel Schwarz, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2018.

– **Loss-of-coolant accidents**

This was the first safety issue pursued in research and development even before the 1970s. The study of loss-of-coolant accidents (LOCAs) that may result from a break in the reactor coolant system is examined in Chapter 9. As explained previously, the decrease in system pressure and the loss of coolant would result in heating of the fuel rods due to decay heat coming from the fuel, even though reactor trip, which automatically drops the rod cluster control assemblies, would interrupt the nuclear chain reaction. This heating phenomenon must remain limited to ensure that fuel damage does not prevent reactor core cooling, thus leading to core melt. Loss-of-coolant accidents contribute to defining the design basis of the safety (water) injection system (flow rate, etc.), certain mechanical components of the reactor coolant system and the reactor containment.

In the 1970s, safety criteria for fuel rod cladding (the first confinement barrier) were defined based on the state of knowledge at the time. These criteria are specified in US regulations, specifically 10 CFR (Code of Federal Regulations) 50.46 and its Appendix K, issued in 1974, which served as the basis for construction of the first nuclear power reactors built in France under license from Westinghouse. The publication of this text was the culmination of years of discussions between the Atomic Energy Commission, forerunner of the U.S. NRC, and U.S. nuclear operators. However, since 1974, reactor operating conditions and fuels have changed (increased burnup rates, new materials for fuel rod cladding, etc.), leading to the implementation of various research and development programmes described below.

There are two major lines of research on loss-of-coolant accidents:

- two-phase thermal-hydraulic phenomena occurring during draining of the reactor coolant system, core reflooding and rewetting of fuel rods,
- the behaviour of cladding and fuels under such accident conditions.

Knowledge of these phenomena has advanced significantly over the last 40 years. It has resulted in the development of sophisticated thermal-hydraulic simulation software, such as the CATHARE system code (see Chapter 40), used to study how these accidents progress at the reactor level and to verify that safety criteria are met within sufficient margins, given the remaining uncertainties.

For this reason, many analytical tests were performed as part of development of CATHARE. Most of them took place between the 1980s and 1990s in special, highly instrumented facilities built by CEA at its Grenoble site. In the 1980s, however, in order to verify the ability of CATHARE software to satisfactorily predict the behaviour of a nuclear steam supply system in an accident situation, CEA, with support from EDF, Framatome and IPSN, designed the BETHSY facility, built at the Grenoble research centre and described in the Focus feature below. In total, more than 80 tests were carried out between 1987 and 1998. They were not limited to the study of a guillotine break ('large break') on a reactor coolant pipe. Other accident situations or phases were studied, such as those that may result from small or intermediate breaks, or from injecting nitrogen into the reactor coolant system after the accumulators have been completely drained, or from a loss of cooling during shutdown when the reactor coolant system is partially drained. The test facility was also used to validate the operating procedures developed as part of the new approach, known as the state-oriented approach (SOA).

Research into fuel rod behaviour during a loss-of-coolant accident has focused mainly on the following phenomena:

- steam oxidation of zirconium alloy cladding, which changes the mechanical properties of the material and produces hydrogen as well as heat,
- swelling and failure of the cladding,
- mechanical resistance of oxidized cladding to the thermal shock induced by reflooding the cladding and to other stresses that may occur during core cooling over the longer term,
- behaviour of fuel pellets inside 'ballooned'[1024] cladding, knowing that these pellets are subject to fragmentation under the stresses generated by normal reactor operation.

The many research and development projects include tests carried out in the 1980s in the EDGAR facility at CEA's Saclay site to study fuel rod mechanics under LOCA conditions. Approximately 500 tests were performed on tubes made from different zirconium alloys, heated directly by the Joule effect. This heating method ensured that the temperature was evenly distributed throughout the tube. The tests established the laws of creep and elongation at break as a function of tube temperature and the rising temperature and pressure ramps. These laws were inserted in the CATHARE system code.

Elsewhere, more recent tests conducted between 2003 and 2012 on single rods in the reactor at the Halden site in Norway (as part of the HRP[1025] LOCA programme sponsored by the OECD/NEA) showed that when the cladding failed, fuel fragments (due to irradiation-induced cracking) moved around inside the rods, entrained by rod depressurization, and that some of the fuel could be ejected outside the rods.

To date, no full experiment has been conducted in a reactor using an irradiated fuel rod assembly. In order to advance knowledge, particularly on the risk of fuel ejection from a rod, IRSN, with support from EDF and the participation of

[1024] Swelling due to heating and the drop in pressure in the reactor coolant system.

[1025] Halden Reactor Project.

the CNRS, launched the PERFROI[1026] research programme in 2013. This six-year programme is co-funded by the French National Research Agency (*Agence nationale de la recherche*, ANR), as part of the Investments for the Future Programme and more specifically the call for proposals for nuclear safety and radiation protection research (*Recherche en matière de sûreté nucléaire et radio-protection,* RSNR), launched in 2012 following the Fukushima Daiichi nuclear power plant accident. This research focuses on the study of blockage between rods (due to cladding swelling, etc.) and whether rods can be cooled when the reactor core is reflooded. They include experimentation and modelling work required to validate the DRACCAR simulation code (see Chapter 40) by 2020. The programme has two main areas of research: the mechanical properties of cladding and two-phase flows.

Finally, as indicated in Section 9.1.4, in the event of a failure in the reactor coolant system of a pressurized water reactor that is not compensated by the chemical and volume control system (CVCS), the core would be cooled by the safety injection system (SIS) and the containment by the containment spray system (CSS). Both systems are first supplied with water directly from the refuelling water storage tank; when it is empty, they are connected to the containment sumps into which water from the break has been discharged, thus operating in 'recirculation' mode. This 'recirculation' cooling mode may be required for a very long time to ensure cooling of fuel assemblies. The reliability of this cooling mode is fundamental to avoid damage to fuel assemblies and core melt.

As indicated in Section 9.1.4, while studies and R&D work have led to changes throughout the nuclear power plant fleet, studies are on-going, particularly on 'downstream' effects. EDF has a work programme and, since 1999, IRSN, together with the company VUEZ and the University of Trenčín in Slovakia, has carried out studies and research in experimental facilities, including the VIKTORIA loop inaugurated in 2011 (see the Focus feature below). This work covers the following topics:

- efflorescence of debris from insulating materials under the effect of water flow;
- vertical transport of debris and crushing of debris through contact with obstacles;
- horizontal transport rates of debris and its sedimentation in the containment;
- filter clogging mechanisms;
- chemical reactions that may occur within the fibrous beds deposited on the filters due to the presence of sodium hydroxide, boric acid and other

[1026] The name is taken from the French *perte de refroidissement*, i.e. 'loss of cooling'.

elements; this includes zinc oxides from the leaching of galvanized gratings by run-off water, which is likely to promote the formation of precipitates (gels and crystals);

- physical and chemical effects downstream of the filters, with characterization of the debris passing through the filters (quantity, type, size) and their effect on fuel assemblies and other components (heat exchangers, diaphragms, etc.).

– **Insertion of reactivity in the core**

As in the case of loss-of-coolant accidents, R&D carried out on reactivity insertion accidents aims to improve assessment of fuel rod resistance and, in the event of fuel rod failure, assessment of the core cooling capacity. From an operational viewpoint, the focus is placed on the reactor trip activation thresholds, which must be determined by taking into consideration current knowledge and remaining uncertainties.

Since the late 1960s, experiments have been carried out in the USA on fresh or moderately irradiated fuels in reactors at the Special Power Excursion Reactor Test (SPERT) Facility (1969-1970) and the Power Burst Facility (PBF) at the Idaho National Laboratory (1978-1980). But, in the early 1990s, two reasons, first, the Chernobyl accident, which occurred following a runaway nuclear reaction, and second, the use of gradually increasing fuel assembly burnup rates envisaged by operators, led to questioning the validity of the fuel energy deposition (enthalpy change) criterion during a reactivity transient, which had been established at 280 calories per gram of UO_2 based on the experiments mentioned above. The criterion was revised downwards: in Europe, values of 220 cal/g for fresh fuel and 200 cal/g for irradiated fuel were adopted.

Research programmes were then conducted in Japan and France to improve understanding of the physical phenomena that can lead to a loss of fuel-rod-cladding integrity and the ejection of fuel fragments into the reactor coolant system, which could have an adverse effect on core cooling. IPSN conducted a programme of 14 tests (Cabri REP-Na [1993-2002]) in the CABRI reactor (see the Focus feature below) using fuel rods taken from nuclear power plants where burnup rates were between 33 and 76 GWd/tU. The fuel rods were placed in a test device inside a loop which, at the time, was cooled using liquid sodium. The fact that the tests were performed with sodium circulating around the rods was considered acceptable to study the essentially mechanical phenomena that occur during the first tens of milliseconds of a reactivity injection accident, during which cladding temperature is hardly affected.

More stringent criteria than those indicated above for admissible fuel enthalpy change in the event of a reactivity accident have now been set based on the results of test programmes (see Section 35.2).

To study the phenomena occurring after the first hundreds of milliseconds (when the cladding dries and bursts), as well as the impact on reactor structures of a pressure wave from possible dispersion of fuel in the reactor coolant, IPSN launched a new experiment programme that required revising the design of the CABRI facility. Supported by the OECD/NEA, the CABRI International Program (CIP) is conducted in partnership with EDF and a number of safety organizations and industrial partners from around the world. The programme includes 10 tests in the new water loop that was built in the CABRI facility. The first test was carried out in April 2018 with a highly irradiated MOX fuel rod.

– **Behaviour of steel and concrete structures**

In the past, knowledge acquired through R&D (including non-destructive testing), often driven by anomalies observed on reactor components, led to various changes on reactors in the French nuclear power plant fleet, including changes in the type of materials used (for example, the discontinued use of Inconel 600), changes in system design (to reduce the risks of thermal fatigue caused by a mix of liquid jets at different temperatures) and enhanced in-service inspections, to name a few. Of course, they also contributed to more in-depth analysis results for safety demonstrations (involving, for example, the performance of reactor vessels subject to neutron irradiation).

The scale of R&D stepped up even further after EDF stated its intention to continue operating reactors beyond 40 years (through its Operating Lifetime Project). Three EDF initiatives in R&D on the ageing of steel and concrete structures are particularly noteworthy:

- creation of the Materials Ageing Institute (MAI);
- the French National CEOS.fr Project (*Comportement et évaluation des ouvrages spéciaux: fissuration – retrait* [Behaviour and Assessment of Special Structures: Cracking and Shrinkage], 2008-2014);
- the VERCORS project, for realistic verification of reactor containments, which began in 2013 with completion expected by 2021, is a major R&D project on reactor containments. Its purpose is to acquire a certain amount of knowledge to support the safety demonstration for accepting a 60-year operating lifetime for reactor containments.

Given the important role of proven or potential pathologies on the 'durability' (lifespan) of reinforced concrete structures and given the extension of the operating lifetime of reactors in the French nuclear power plant fleet, IRSN considered that it would be appropriate to establish an 'observatory' on the durability of nuclear civil works in cooperation with scientific partners and to share knowledge on the ageing of these structures and the potential problems that could occur. Initiated in 2014, the project was named ODOBA (*Observatoire de durabilité des ouvrages en béton armé* – Observatory of Durability in Reinforced Concrete Structures). It studies pathologies affecting civil works (presented in

Section 27.6.1), such as corrosion of reinforcement bars, concrete swelling (due to reactions such as delayed ettringite formation and alkali-silica reaction), and their impact on safety.

Knowledge will be acquired concomitantly with the assessment of plans to extend the service life of French nuclear power plants beyond 40 years.

The experimental portion includes the construction, at the Cadarache research centre, of concrete components representative of the concrete used to build reactor containments in the nuclear power plant fleet. The components (about sixty blocks), one metre thick – and a few metres in height and width – will undergo either an accelerated ageing process, or a natural ageing process, in order to establish a basis of equivalence with accelerated ageing.

In 2015, the U.S. NRC joined the project.

– **Core melt**

The numerous topics that question and examine core-melt situations are approached in Chapter 17, which discusses the risks associated with hydrogen production and basemat melt-through caused by interaction between molten materials (corium) and the basemat. Research on these subjects has led to installing passive autocatalytic recombiners on reactors in the French nuclear power plant fleet, adding thickness to the basemat of the Fessenheim nuclear power plant (the same process also being applied to other reactors), implementing specific measures to manage core-melt situations and issuing a severe-accident operating guide.

More recently, a measure envisaged by certain designers and operators to prevent vessel breach due to core melt consists of flooding the reactor pit in order to cool the vessel using a two-phase flow of water around it and thus retain the corium in the vessel lower head (In-Vessel Retention – IVR). This possibility, if tried and proven, would reduce the risk of containment failure (less hydrogen produced, no corium-concrete interaction). The effectiveness of this action depends, however, on many factors, including the size and power of the reactor, the moment when materials move to the bottom of the vessel, the fraction and composition of the corium in the vessel lower head, which determines the distribution of the heat flux applied to the inner wall of the lower head[1027], as well as the geometry of the reactor pit and the thermal insulation characteristics of the vessel. It is also important to consider the possible presence of geometrical singularities (discontinuous thickness at the junction between the vessel side wall and lower head, instrument penetrations in the lower head) which determine the heat flux that can be removed through the outer surface of the vessel, into the water.

[1027] It is possible that a focusing effect of the lateral heat flux occurs on the upper part of the corium.

A strategy of in-vessel retention has been adopted for certain reactors (the Russian VVER 440/213 reactor, the American AP600 and AP1000 reactors, the South Korean APR-1400 reactor and the Chinese CPR-1000 and CAP1400 reactors).

Initiated in 2015, the European In-Vessel Melt Retention (IVMR) project brings together IRSN (project lead), EDF, Areva (Framatome since 2018), Tractebel Engineering, the Joint Research Centre (JRC), ŬJV Řez in the Czech Republic and 17 other European partners. The aim of the project is to analyse the technical feasibility of the 'IVR strategy' for high-power reactors, including both existing reactors (such as the VVER-1000/320) and different types of future reactors (pressurized water reactors and boiling water reactors).

The Phébus Fission Products (FP) international research programme, which took place from 1988 to 2010, made a major contribution to knowledge of the phenomena involved in a core-melt accident, particularly regarding the potential release of radioactive substances to the environment. These tests were carried out in the PHEBUS reactor, a facility reproducing a 900 MWe reactor on a scale of 1:5000. Testing proceeded by placing a test device (usually a test cluster) at the centre of the PHEBUS reactor (see the Focus feature below) where there was a sealed cylindrical cavity into which was inserted the test device containing in most cases a test cluster. The cluster consisted of 18 irradiated fuel rods and two instrumented fresh rods. In the centre there was a rod simulating the components of a rod cluster control assembly. The reactor coolant system contained a steam generator simulated by an inverted U-tube. The containment was simulated by a 10 m^3 tank comprising a water-filled space (representing the reactor sump), a gas-filled space and painted surfaces.

A test was conducted in two successive phases:

- a 'degradation phase', lasting a few hours, during which, by gradually increasing the power of the PHEBUS reactor core, the temperature of the test fuel rods rose until the materials were liquefied and displaced (between 2300 and 2500°C), causing release of fission products, which were then transported into the system and tank; at the end of this phase, the PHEBUS reactor was shut down;
- a 'containment phase' of several days, during which quantities that are useful in understanding transport and deposition phenomena, as well as iodine chemistry in the system and the tank, were measured.

The various tests conducted during the Phébus-FP programme provided scientific information on core melt, aerosol composition, the lower-than-expected retention of aerosols in system lines, revaporization of certain fission products and hydrogen production. Observations showed that for a reactor equipped with control rods made of a silver-indium-cadmium alloy, the reactor coolant system was the main source of volatile iodine in the containment. For boron carbide control rods, the release of gaseous iodine was greater. The test programme clearly demonstrated a link between fuel degradation phenomena and fission product release kinetics. In addition, the programme showed that beyond 24 h, the concentration of volatile iodine in the tank simulating the containment depends mainly on physical-chemical processes in the gas phase. It therefore depends on the concentration of volatile iodine coming from the reactor coolant system or formed in the containment, which in turn depends on whether the iodine is attracted to the containment surfaces (paint, material, etc.).

The sequence of events that occurred during the core-melt accident at the Fukushima Daiichi nuclear power plant drew attention to the benefits of equipping the containment filtered venting systems (in France, the U5 device equipped with a metal pre-filter and a sand filter) with innovative filtration devices for capturing all volatile forms of iodine. Supported by the EU Commission, the Passive and Active Systems on Severe Accident source term Mitigation (PASSAM) project brought together nine partners, including IRSN (project lead), EDF, Areva and the Paul Scherrer Institute (PSI) in Switzerland, to explore possible improvements to reactor filtration systems and study innovative devices for greater efficiency. The project, launched in 2013, was completed in 2017. Several existing devices were reviewed (sparging filters, sand filters and metal pre-filters) as well as several innovative systems (high-pressure sprayers, electrostatic precipitators, 'advanced' zeolites[1028], acoustic agglomeration systems and combined wet and dry filtration systems). Findings from the experiments conducted during the PASSAM project have led to the development of new computational models as well as improvements to existing models. These models are used in severe accident computational software, including ASTEC software (see Chapter 40) and computational software specific to sparging devices.

- **Phenomena that may occur when fuel assemblies in a spent fuel pool are uncovered**

  Safety issues related to fuel storage in spent fuel pools are discussed in Chapter 15. The loss of fuel assembly cooling, possibly due to water drainage, is a major safety issue; failure to provide sufficient cooling of the assemblies could lead to the anticipated 'cliff-edge' effect, consisting of runaway exothermic oxidation reactions from the fuel rod cladding exposed to air and water vapour, leading to cladding degradation, ignition of the zirconium and significant release of radioactive substances. While the release would contain very little radioactive iodine-131, given the amount of time the fuel is stored after being discharged from the reactor core, it would most probably contain a very large amount of ruthenium, a particularly radiotoxic element – even though it has a significantly lower half-life than that of caesium.

[1028] Crystals formed from a microporous skeleton of aluminosilicates. These porosities with a discriminant power of less than 100 picometres (10^{-10} m) may or may not prevent molecules from passing. This is why zeolites are referred to as molecular sieves.

While measures are taken to 'practically eliminate' the possibility of an unacceptable loss of cooling (sufficient to lead to uncovery of fuel assemblies), research is nonetheless being conducted to mitigate this risk – given the considerable impact that this loss-of-cooling event could have.

Therefore, in 2013, in cooperation with the CNRS, IRSN launched the DENOPI programme on accidental uncovery of nuclear spent fuel pools. This six-year programme was co-funded by the French National Research Agency (ANR) as part of the Investments for the Future Programme, as well as the call-for-projects for nuclear safety and radiation protection research launched in 2012 following the accident at the Fukushima Daiichi nuclear power plant. It includes carrying out experiments – as well as modelling and validation of simulation software (such as DRACCAR) – to deepen understanding of the different phases in a loss-of-cooling accident or accidental uncovery of fuel assemblies stored in a spent fuel pool. It is based on an analytical approach that aims to develop knowledge on the following three subjects:

- cooling by natural convection at the scale of the pool; this subject is studied using a 1:5 scale mock-up of a pool;
- the thermal-hydraulic behaviour of a fuel assembly in the event of uncovery and the effectiveness of water spraying; this subject is studied using a full-scale mock-up of a fuel assembly and its storage cell under conditions representative of the different accident phases, i.e. loss of cooling, pool water boiling, uncovery and resumption of cooling;
- the fuel cladding oxidation acceleration mechanisms in the presence of a mixture of air and water vapour, the phenomena of cladding oxidation and runaway, as well as the presumed role of nitrides are studied using high-performance laboratory techniques.

– **Earthquakes**

Research and development conducted on hazards generally benefit all types of nuclear facilities.

The Tohuku earthquake in Japan on 11 March 2011 and the subsequent tsunami that affected the Fukushima Daiichi nuclear power plant, the July 2007 tsunami at Chūetsu-oki near the Kashiwasaki-Kariwa[1029] nuclear power plant and, to a lesser extent, the August 2011 tsunami in the US state of Virginia, approximately 18 km from the North Anna nuclear power plant[1030], highlight the limits of knowledge and methods that serve as input in designing nuclear facilities. There is now a broad international consensus on the need to expand this knowledge and the assessment of natural hazards that can seriously affect nuclear sites. This is particularly true in France, where improving consideration

[1029] There was no damage to the plant.

[1030] The earthquake, of moderate magnitude (5.8) and shallow depth (6 km), was not expected given the historical seismicity of the affected part of Virginia.

of seismic risk (and flooding risk) has been one of the priorities identified in operating experience feedback from the Fukushima Daiichi nuclear power plant accident and is reflected in the calls for projects for nuclear safety and radiation protection research by the French National Research Agency (ANR) with funding from the Investments for the Future Programme.

In this new context, the definition of 'extreme' hazards leads to two types of studies: one related to the knowledge of phenomena (including historical records), the other devoted to developing methods for taking them into account, along with the corresponding uncertainties.

Within this context, the goal of the SINAPS@[1031] research project[1032] (2013-2019) was to assess seismic risk in its entirety, from ground faults to civil works and equipment. It aims to explore the uncertainties inherent to assessing seismic hazards and the vulnerability of structures and equipment. The main objective is ultimately to identify, and even quantify, the seismic margins that result from design choices and dimensioning studies (materials, earthquake-resistant construction measures, design assumptions and criteria, etc.).

Since the early 1980s, studies and research have also been carried out in the field of human and organizational factors. At the outset, research work focused on issues concerning the ergonomics of nuclear reactor control rooms and the development of computerized operating procedures. The increasing use of subcontracting has become another topic of research. In addition, since the Fukushima Daiichi nuclear power plant accident and the lessons learned from this event, research is being conducted on emergency response management in extreme situations (EDGE project[1033]), as well as topics in the human and social sciences concerning risk 'governance' (AGORAS project[1034]).

Research also involves the development of new technologies to improve nuclear safety. The following can be cited as examples:

[1031] *Séisme et Installation Nucléaire : Améliorer et Pérenniser la Sûreté* – Earthquakes and Nuclear Facilities : Ensuring and Sustaining Safety.

[1032] CEA is the coordinator for the project, which also includes EDF, IRSN, the French Institute of Science and Technology for Transport, Development and Networks (IFSTTAR), the *École centrale de Paris* and *ENS Paris-Saclay* (formerly the *École nationale supérieure de Cachan*).

[1033] The goal of the EDGE project (for interfacing expertise and decision-making in emergency response situations in high-risk industries – 2016-2019), led by IRSN and conducted in partnership with INERIS, was to understand how emergency response organizations foster cooperation among stakeholders to deal with an unforeseen event that could potentially put the population at risk. The project focused particularly on understanding how these organizations facilitate technical assessments conducted by local and national public services during industrial accidents.

[1034] AGORAS: *Amélioration de la gouvernance des organisations et des réseaux d'acteurs pour la sûreté nucléaire* (Improving the Governance of Organizations and Stakeholder Networks in Nuclear Safety). This project (2014 to 2019) was selected at the end of 2013 in response to the call for projects on nuclear safety and radiation protection research (RSNR) launched by the French National Research Agency (ANR). IRSN participated in this project on risk governance and emergency response management. It is coordinated by *Mines ParisTech* and *École des mines de Nantes* as well the Centre for the Sociology of Organisations at Sciences Po.

- work carried out under the PASSAM project mentioned above on research into filters that are more efficient than the current containment filtered venting devices,
- work carried out jointly by CEA and IRSN on new 'conformable' ultrasonic transducers for in-service inspections of metal parts with complex shapes, etc.

Research topics thus cover a wide range of fields, from equipment to human behaviour, from fuel performance to containment behaviour, from reactor to spent fuel pool, from the facility to the natural environment in which it is located and from design to operational response conditions and facility operation.

39.2.2. Dedicated frameworks and organizations involved

In France, the main organizations conducting research in nuclear safety are the French Alternative Energies and Atomic Energy Commission (CEA), EDF, IRSN (previously IPSN) and the designer Areva (Framatome before 2006 and again after 2018), bearing in mind that many research projects involve partnerships between these entities[1035] and other international actors. Gaining a deeper understanding of the basic science at work in these issues also increasingly involves the world of academic research: universities, engineering schools and the French National Centre for Scientific Research (CNRS).

The nuclear safety research subjects studied by IRSN[1036], alone or in partnership, are part of scientific strategies and programmes that aim to build its assessment and response capabilities, for example in emergency situations, on a solid foundation of scientific knowledge. These scientific strategies and programmes are naturally shaped by safety analyses, changes in reactor design, lessons learned from operating experience (particularly from incidents), accidents (Three Mile Island, Chernobyl and Fukushima Daiichi), as well as findings from previous research. They address subject matters considered to be the most sensitive and the most promising in terms of safety; some of them are forward-looking, and may even aim to propose incentives to operators and designers by revealing and characterizing certain risks to facility safety and providing experimentally proven facts on the possible safety benefits of innovative systems, etc.

The complexity of experimental equipment to be designed and implemented – in particular systems to be installed in nuclear research reactors such as CABRI and PHEBUS – and the time required for examinations or post-testing in specialized

[1035] Partnerships between EDF, Framatome, CEA and IRSN are defined within the framework of steering committees and can take various forms, including joint work limited to a few partners on subjects of common interest.

[1036] Readers may wish to refer to IRSN's scientific strategy document, released in October 2015: https://www.irsn.fr/EN/Presentation/governance/Documents/scientific-strategy-2015/index.html#page=1. CEA's press kit *Les recherches du CEA sur la sûreté nucléaire* (CEA Research on Nuclear Safety, February 2012) presents some of its key research topics in light of the Fukushima Daiichi nuclear power plant accident.

laboratories, especially when radioactive material is used during the tests, means that a considerable amount of time may be spent (more than ten years in some cases) before results relevant to safety analysis are obtained. It is therefore important to identify at a sufficiently early stage the knowledge required and the simulation software needed to be ready for facility milestones such as periodic reviews.

Because of the cost, a large number of these research projects, particularly those involving experimentation, are conducted within cooperative frameworks, where each partner (inside or outside France) is free to use the research findings – and all partners keep each other informed on their developments, another advantage of collaborative work. The other main countries that have designed and built nuclear power reactors (USA, Canada, Japan, Germany, United Kingdom, Switzerland, Russia, etc.) have conducted and continue to conduct nuclear safety research programmes with French partners.

In France, research projects are financed by the French National Research Agency (ANR), for example, as part of the call for research projects in nuclear safety and radiation protection (RSNR) after the Fukushima Daiichi nuclear power plant accident – some of which were cited above.

The European Commission also makes a significant contribution to funding international research and development projects in nuclear safety. Since 1984, the Commission has issued calls for projects as part of Euratom's multi-year Framework Programmes for nuclear research[1037]. The projects selected are carried out in a variety of cooperative frameworks, most often bringing together industry, nuclear power plant operators, assessment organizations and research laboratories.

The Nuclear Energy Agency of the Organisation for Economic Co-operation and Development (OECD/NEA) plays an important role in research by developing and disseminating state-of-the-art reports, which identify gaps and priorities for research. Internationally, it organizes benchmark exercises to compare different simulation software packages with experimental findings (International Standard Problems or ISPs); these exercises always provide very rich insights. It also facilitates the preparation of international research projects[1038].

Two books examine these subjects in detail:

- a general work, Current State of Research on Pressurized Water Reactor Safety, Science and Technology Series, IRSN/EDP Sciences, 2017, which gives a detailed presentation of the history and state of this research (and developments) on

[1037] In 2007, a European organization composed of experts from various sectors of the nuclear industry, including fusion reactors and associated fuel cycle facilities, was set up to assist the European Commission in the selection and prioritization of important research and development topics: the SNETP (Sustainable Nuclear Energy Technology Platform). In 2012, SNETP was enlarged to create NUGENIA (NUclear GENeration II & III Association), a Belgian non-profit organization. These organizations have issued several strategic documents.

[1038] For further information, see Main Benefits from 30 Years of Joint Projects in Nuclear Safety, OECD/Nuclear Safety, 2012.

several important topics, with questions and issues that still require further knowledge; and

- Nuclear Power Reactor Core Melt Accidents – Current State of Knowledge, Science and Technology Series, IRSN/EDP Sciences, 2015.

39.2.3. Facilities in France used for research and development

The following Focus feature presents some of the research facilities operating in France.

#FOCUS

Examples of French research facilities

It is not possible to present, even briefly, all the facilities and systems devoted to R&D that has been conducted for over forty years on safety issues pertaining to pressurized water reactors; the following list is therefore necessarily incomplete.

In France, the development and deployment of pressurized water reactors benefited from the results of numerous R&D projects involving experiments conducted on various types of research reactor[1039] (ranging from very low-power critical mock-ups – some air-cooled – to pool-type reactors producing a few tens of megawatts) to acquire knowledge on reactor physics and the behaviour of materials under irradiation. These facilities include the following operated by CEA:

- the critical mock-up facilities called **MINERVE** (started up in 1959) and **EOLE** (started up in 1965), featuring a maximum power of 100 W. Experiments in these reactors ended in late 2017; the ZEPHYR facility project is under way to succeed them;
- the **SILOE** pool-type reactor at the CEA Grenoble site, operated from 1963 to 1997 at a power of 35 MW;
- the **OSIRIS** technological irradiation reactor at CEA Saclay was in operation from 1966 to 2015. It was a pool-type reactor, cooled and moderated using light water; the neutron fluxes inside the core or at its periphery were higher than those in a pressurized water reactor, making it appropriate for accelerated study of materials ageing under irradiation in this type of reactor. It also

[1039] For more details on this type of reactor, see Research Nuclear Reactors (a Nuclear Energy Division monograph, CEA – *Éditions Le Moniteur*, 2012), and Elements of Nuclear Safety – Research Reactors, Science and Technology Series, IRSN/EDP Sciences (2019). See also at the following link: http://www.materials.cea.fr/en/PDF/Research%20nuclear%20reactors_CEA-en.pdf.

served to produce artificial radioisotopes used in medicine for scintigraphy diagnostics and treating certain pathologies;

- **Jules Horowitz Reactor** (**RJH**). This pool-type reactor is under construction at the CEA Cadarache site. It will replace the OSIRIS reactor and will generate 100 MW of power. It includes a 'travelling' telescopic system that will be used to study the effect of power transients on fuel rods (see Figure 39.1).

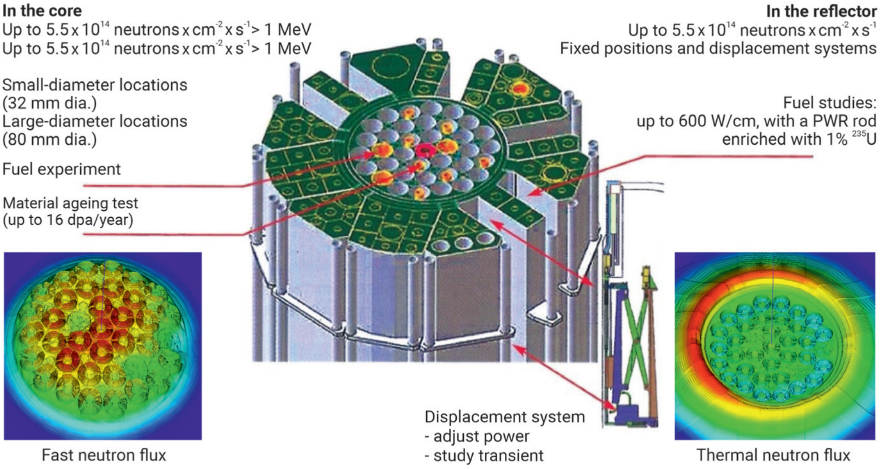

In the core
Up to 5.5 x 10^{14} neutrons x cm^{-2} x s^{-1} > 1 MeV
Up to 5.5 x 10^{14} neutrons x cm^{-2} x s^{-1} > 1 MeV
In the reflector
Up to 5.5 x 10^{14} neutrons x cm^{-2} x s^{-1}
Fixed positions and displacement systems
Small-diameter locations
(32 mm dia.)
Large-diameter locations
(80 mm dia.)
Fuel experiment
Material ageing test
(up to 16 dpa/year)
Fuel studies:
up to 600 W/cm, with a PWR rod
enriched with 1% ^{235}U
Displacement system
- adjust power
- study transient
Fast neutron flux
Thermal neutron flux

Figure 39.1. Jules Horowitz Reactor: diagram showing the core and the 'reflector' zone for different experimental uses; neutron flux in the different zones is indicated. CEA.

More specifically in terms of safety, the **BETHSY** thermal-hydraulic test loop at the CEA Grenoble site played an important role in the study of loss-of-coolant accidents in a pressurized water reactor. More than 80 tests were performed there between 1987 and 1998, with support from EDF, Framatome and IPSN. This was a mock-up of the reactor coolant system in a 900 MWe reactor at full scale in terms of component height, with a volume scaling ratio of 1:100. It consisted of three loops, each equipped with a pump and a steam generator, as well as those secondary system components considered essential for thermal-hydraulic studies. The reactor core was represented at a scale of 1:100 by an assembly of 428 rods, clad in stainless steel and heated electrically. They were capable of generating 3 MW, which represents about 10% of the nominal power of a reactor of this scale, making it possible to simulate residual heat in the core just after the rod cluster control assembly drop. All the safety systems were modelled, including the high- and low-head injection systems, accumulators, and secondary system valves. Breaks could be simulated at various points in the reactor coolant system: in the cold and hot legs, at the top of the pressurizer and in the steam generator. More than 1000 measurement channels were used to monitor changes in key parameters (temperature, pressure, flow rate and direction, void fraction, etc.)

during tests. The tests carried out in the BETHSY loop contributed to validation of the CATHARE simulation system code and accident operating procedures.

Among the experimental facilities outside France dedicated to the study of thermal-hydraulic behaviour of nuclear steam supply systems in accident situations, the PKL facility (*Primärkreislauf*, Erlangen, Germany) operated by Areva (now Framatome) is noteworthy: it models on a 1:145 scale the volume and power of a 1300 MWe KONVOI-type reactor designed by Kraftwerk Union (KWU), on a 1:1 scale in terms of height. It is equipped with four loops and has 314 electrically heated rods. Three successive programmes (PKL [2004-2007], PKL-2 [2007-2011] and PKL-3 [2012-2015]) were carried out there to study, among other things, the dilution phenomena of boric acid in various situations (subject covered in Section 35.1.3) and natural convection in the event of loss of cooling during shutdown (and 'in-vessel mixing'[1040] in general), or to simulate beyond-design-basis situations corresponding to delayed startup of safety injection in order to assess safety margins.

The **VERDON**[1041] facility is located in two 'hot cells' located in the LECA-STAR laboratory at CEA's Cadarache site. This facility is used to receive and characterize samples of fuel freshly re-irradiated in a research reactor (to reconstitute the inventory of short-lived fission products, which have a preponderant radiological impact); to heat samples in an induction furnace under a controlled atmosphere in order to simulate core-melt accident configurations; and to study fission product releases and their transport in the reactor coolant system of a pressurized water reactor. The purpose of this research work is to identify fission products released in the event of an accident and contribute to a better understanding of their physical-chemical form in order to improve equipment used to reduce the release of radioactive substances to the environment in accident situations.

The experiment programme associated with the **MISTRA** facility at CEA Saclay aims to study thermal hydraulics in a pressurized water reactor containment in core-melt situations, particularly the risks associated with hydrogen released in the containment. Its objectives are:

- to understand the thermal hydraulics of this type of accident and the dispersion of hydrogen in a confined environment,
- to study different mitigation strategies (inerting and use of recombiners).

The MISTRA facility represents a single PWR containment at a 1:10 scale (see Figure 39.2). The vessel is made of stainless steel and is thermally insulated using a 20 cm layer of rock wool. Before the experiments begin, the facility is preheated using steam injection and condensation; thermal inertia is sufficient

[1040] Combinations of volumes of water at different temperatures and boron concentrations.

[1041] The following information on CEA facilities is taken from the press kit *Les recherches du CEA sur la sûreté nucléaire* (CEA Research on Nuclear Safety), February 2012.

to stabilize the external wall temperature. The facility includes several gas and steam injection systems. Mass flows of gas injection are controlled and measured using sonic throats that keep values constant regardless of downstream operating conditions.

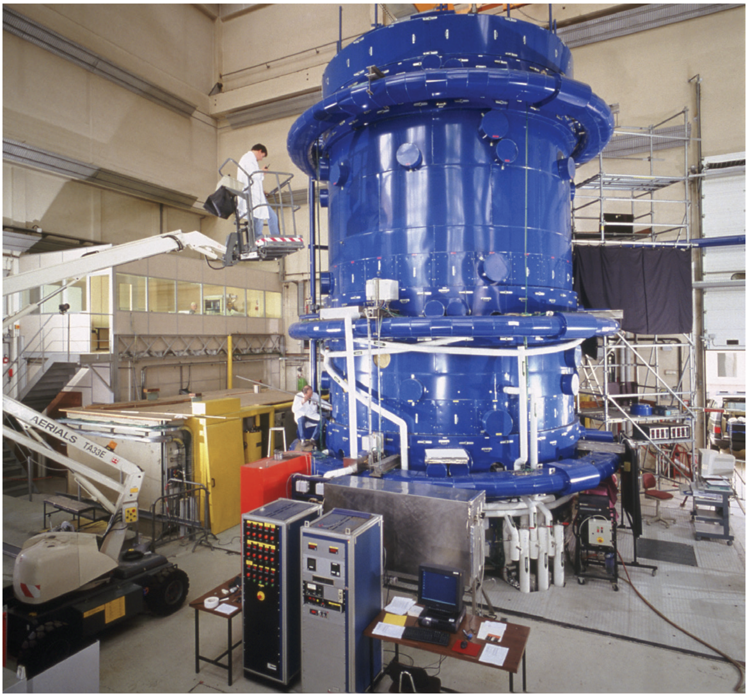


Figure 39.2. View of vessel at the MISTRA facility. A. Gonin/CEA.

CEA’s **PLINIUS** experimental platform at the Cadarache site is the only European platform devoted to the study of severe accidents using large masses of ‘prototypical’ corium (high-temperature molten mixtures containing [depleted] uranium oxides, which are characteristic of the molten mixtures that could form in the event of a light water reactor core-melt accident). The platform consists of four facilities:

- **VULCANO,** featuring a furnace in which 50 to 100 kg of corium can be melted. The molten corium is poured into a specially instrumented test section (either a spreading test section or a crucible);
- **KROTOS,** a facility designed to study thermodynamic interactions between molten materials and a coolant (steam explosions). In this facility, 4.5 kg of corium or 1 kg of alumina can be melted and poured into a test section filled with water in order to study the premixing and explosion phases (see Section 40.4). Spontaneous explosions have been observed;

- **COLIMA**, a facility in which a few kilograms of corium can be melted by induction heating. The crucible is installed in a 1.5 m^3 vessel. The temperature of the vessel walls can be controlled up to 160°C. The facility can be used to simulate a core-melt accident in a light water reactor and its consequences on the containment atmosphere (composed of air and water vapour at a pressure of 5 bars and a temperature of 150°C);
- **VITI,** a 'high-temperature' facility designed to study material properties, mainly viscosity and surface tension. In this facility, (depleted) uranium can be used in the corium. Induction is used for contactless heating and taking measurements on samples.

Another CEA facility at the Saclay site is the **TAMARIS** facility equipped with the **AZALÉE** vibrating table, used for seismic risk analysis (see Figure 39.3). For more than 40 years, CEA has conducted seismic engineering studies to understand the behaviour of structures, systems and components under seismic loading using numerical and experimental tools at the TAMARIS facility. The AZALÉE vibrating table is currently the largest triaxial test facility in Europe.

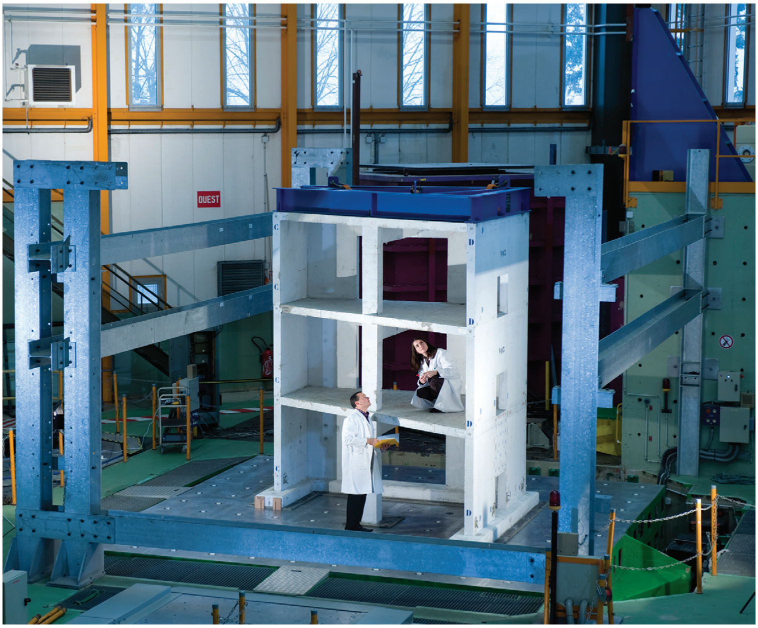


Figure 39.3. View of a nuclear building mock-up (such as an electrical building) for seismic simulation on CEA's AZALÉE vibrating table. P. Stroppa/CEA.

Some of IRSN's more important research facilities are described below.

- The **CABRI** reactor (see Figure 39.4) – operated by CEA and made available to IRSN – is located at the Cadarache site and is used to study the consequences of reactivity accidents on fuel. By depressurizing rods filled previously with a neutron-absorbing gas (^{3}He), the reactor is capable of creating power spikes similar to those that could occur during a reactivity accident in a pressurized water reactor.

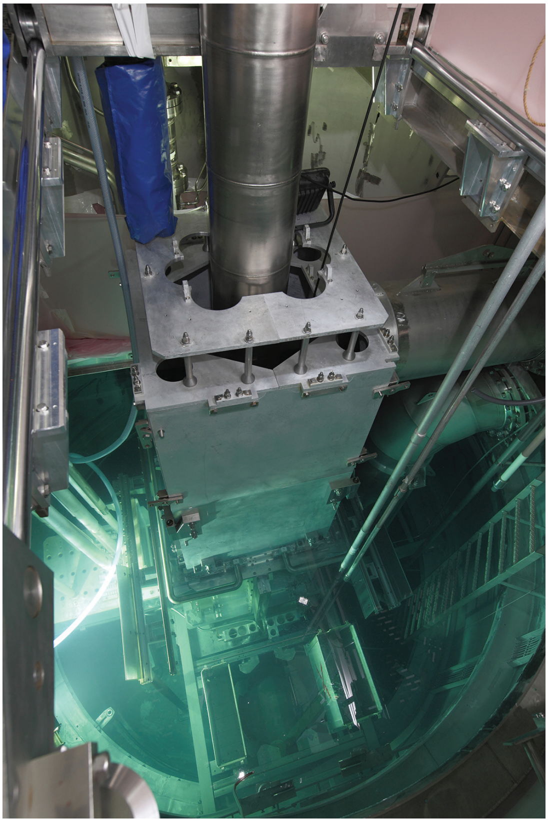


Figure 39.4. Top view of the CABRI reactor core in the water pool and the test loop (containing sodium at the time) that passes through the pool vertically. G. Lesénéchal/CEA.

- The **PHEBUS** reactor at the Cadarache site is operated by CEA and made available to IRSN (shut down since 2010). It was the experimental tool for several experiment programmes, including the Phébus-FP programme mentioned above, used to study what happens to fission products released from a pressurized water reactor core in core-melt situations. These tests contributed to the development and validation of models and computer codes, particularly ASTEC.
- The **TOSQAN** test station for simulation and qualification in airborne conditions (see Figure 39.5) is located at the Saclay site and operated by IRSN. The facility simulates thermal-hydraulic conditions in the containment of a nuclear reactor during a core-melt accident. It is used to analyse the phys-

ical phenomena influencing the distribution of hydrogen in the containment (condensation on walls, exchanges induced by the sump or water spraying system in the containment).

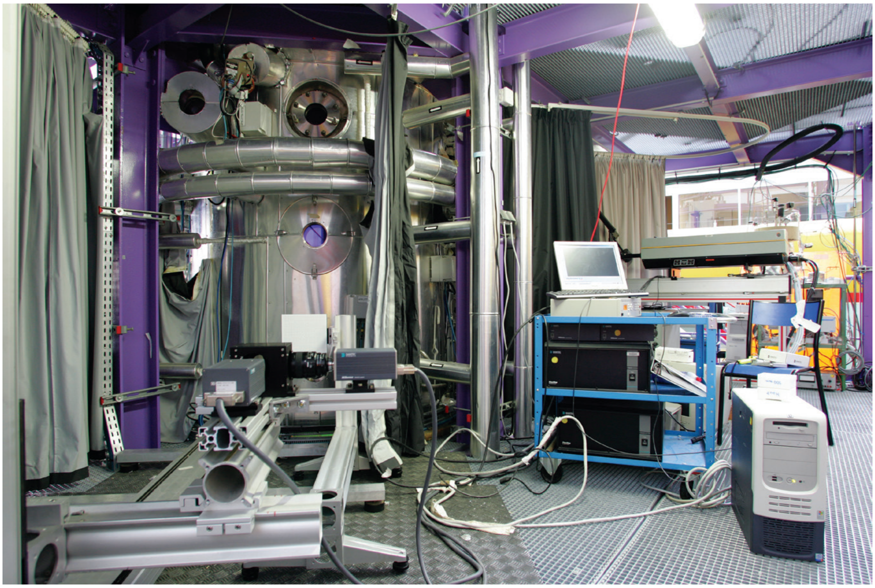


Figure 39.5. View of the TOSQAN facility. Olivier Seignette, Mikaël Lafontan/IRSN Media Library.

- The **CHIP** and **EPICUR** facilities are operated by IRSN at the Cadarache site. The first is used to study the physical-chemical behaviour of iodine in the reactor coolant system of a pressurized water reactor in core-melt situations; the second to study the physical-chemical behaviour of iodine under radiation in the containment in core-melt situations.
- The **PEARL** facility operated by IRSN at CEA Cadarache is used to study the coolability of debris (or corium) beds as part of the European IVMR project mentioned above. It includes (see Figure 39.6) a water tank that can be heated, two water injection lines, a quartz test section (2.66 m high, 540 mm diameter) that contains the instrumented debris bed, a steam discharge line and a pressure control valve. The debris bed consists of metal balls (total mass approximately 500 kg) heated by induction. The plant also includes a steam generator used to create a steam atmosphere in the debris bed before the reflooding phase (water injection). The test section is placed in a 20 m^3 vessel designed to withstand a pressure of 10 bars. The facility is equipped with instrumentation to measure temperature and pressure loss within the debris bed, as well as injected water flow rate, steam flow rate and system pressure.

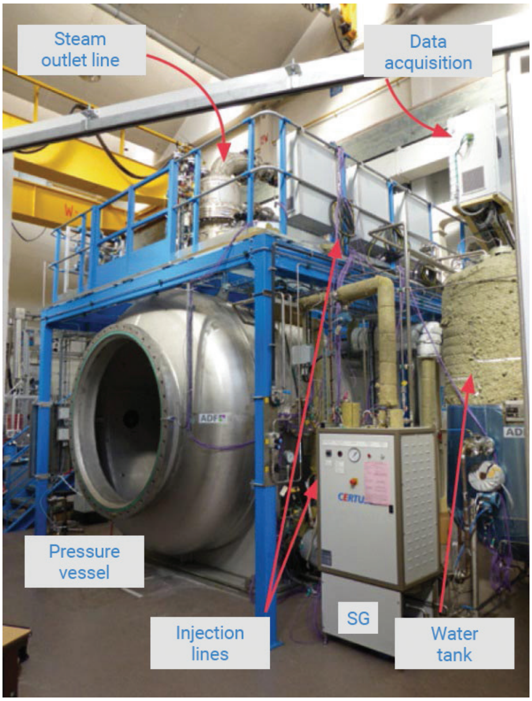


Figure 39.6. View of the PEARL facility. IRSN.

– IRSN operates the **DIVA** facility at the Cadarache site to conduct research on fire, ventilation and airborne contamination. It is used to perform fire tests in configurations involving several ventilated rooms in laboratories and plants as well as nuclear reactors (see Figure 39.7).

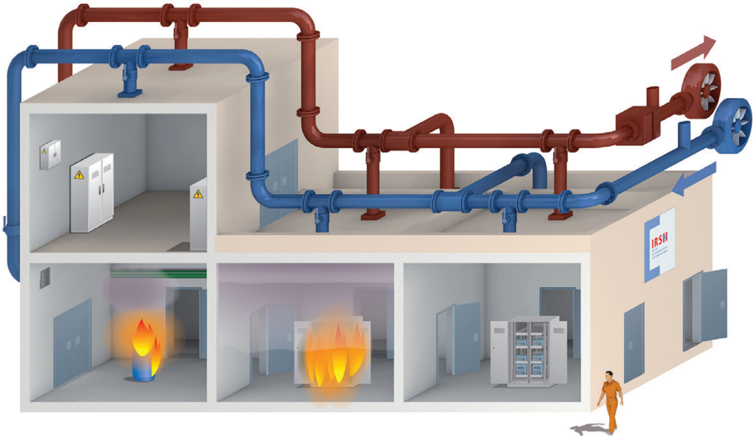


Figure 39.7. Schematic view of the DIVA facility. IRSN.

– The **VIKTORIA** loop, co-funded by IRSN and operated by VUEZ in Levice, Slovakia, is used to study physical and chemical phenomena essential for analysing filtration issues when cooling a reactor by recirculating water in the containment. The loop includes (see Figure 39.8):

- tanks for preparing and keeping debris in suspension before it is transferred to the sump filter under study;
- a channel for transferring debris to the compartment equipped with the filter (1% inclined plane, 2 m long and 0.99 m wide); the height of the water level is used to adjust the speed at which debris is transferred into the channel (approximately 6 cm/s);
- the compartment fitted with the tested filter (the tests were conducted using a CCI cartridge filter made by Areva);
- a downstream zone, featuring two fuel assembly modules.

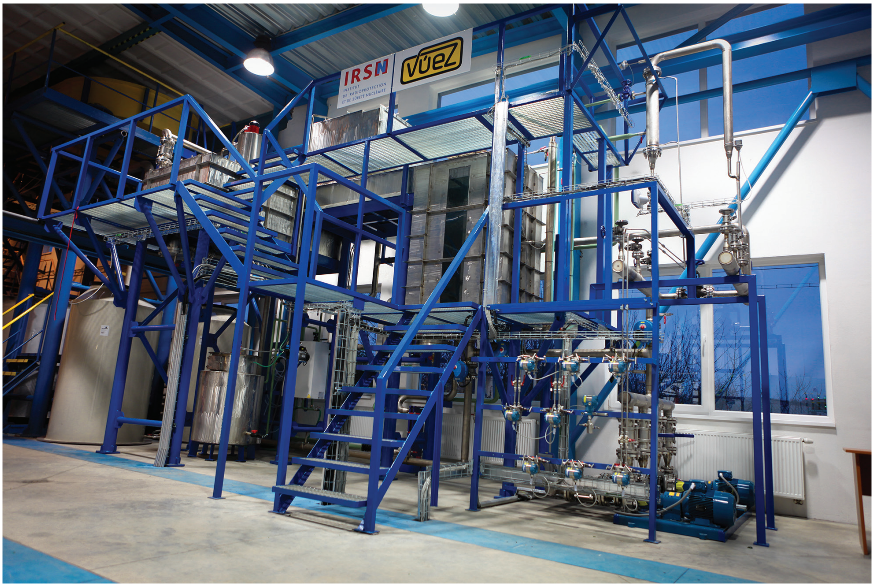


Figure 39.8. View of the VIKTORIA test loop. Brano Valach/IRSN.

The Halden Man-Machine Laboratory (**HAMMLAB**) in Norway is used for experiments involving human and organizational factors (see Figure 39.9). The experiments are carried out within the framework of the Halden Reactor Project, set up in 1958 by the OECD/NEA, which brings together 19 member states that fund research work in fields including nuclear fuel, the behaviour of materials in a nuclear environment, human and organizational factors and human-machine interfaces. Certain research work was carried out directly on a small 20 MW experimental reactor (the Halden Reactor, a boiling heavy water reactor that regularly accommodated about 30 experimental devices simultaneously). The reactor was decommissioned in 2018.

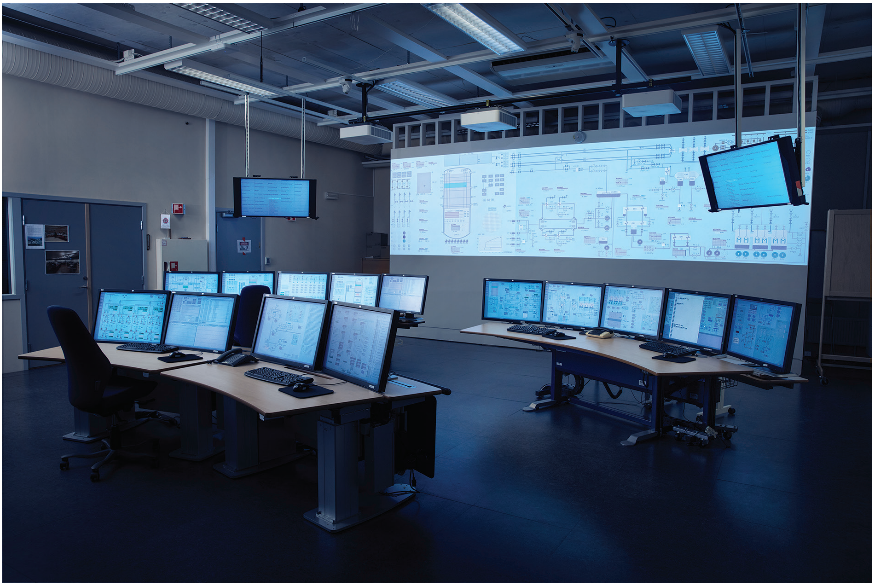


Figure 39.9. The HAMMLAB facility. Espen Solli.

Videos available for viewing

CABRI Reactor

GALAXIE
Experimental Platform

EPICUR Facility

PEARL Facility
(in French)

Chapter 40

Examples of Simulation Software Developed for Safety Analysis of Pressurized Water Reactors

The design and modification of pressurized water reactors as well as their safety demonstration – including the safety reassessment conducted during periodic reviews – are based on studies usually carried out using simulation software in various fields, including neutronics and criticality (core operation and fuel storage), thermal hydraulics (core, cooling systems) and structural mechanics (metal structures, civil works), to name a few. It is primarily the operator, Électricité de France (EDF), who conducts these studies, but IRSN also does so during its assessment of the files that the operator submits to the French Nuclear Safety Authority (ASN).

It is important to validate simulation software before it is used for studies. The ability of each simulation tool or 'code' to accurately or conservatively represent the physical phenomena in question must therefore be established as part of a safety demonstration, or in the expert assessment of this demonstration.

Performing 'integral' tests on mock-ups for demonstration purposes may be desirable, or even essential, to support certain assessments established through calculations, in cases where the assessments involve uncertainty that is too high (including due to modelling simplifications) or when the software has been validated only with its various physical models considered separately. Two examples were mentioned in the Focus feature in the preceding chapter: the tests carried out in the BETHSY loop – which contributed to the overall validation of CATHARE software – and the Phébus-FP programme tests – which contributed to validating ASTEC software.

It is also important to recall the particular importance, in the case of a new reactor (or a reactor that has undergone substantial changes), of startup tests (or restart tests) performed by the operator on various items of equipment or systems to ensure, as far as possible[1042], that they are capable of performing the functions for which they were designed, at the performance levels targeted in design studies, largely based on the use of simulation software.

Some of the simulation codes[1043], in versions that have been improved over time, and their most noteworthy uses for pressurized water reactors in the French nuclear power plant fleet are briefly described below[1044]. Given the very large number of simulation codes used by the designer, EDF and IRSN[1045], this chapter is not intended to be exhaustive; for the most part, it covers codes developed or used by IRSN, although some are also used by the designer or EDF.

The extensive work entailed in developing and validating the simulation codes presented is not covered in this discussion[1046].

40.1. Simulation software for neutronics

- **APOLLO**: this two-dimensional simulation software[1047] used in the field of neutronics is based on neutron transport theory (Boltzmann equation) for a steady (stationary) state capable of simulating fuel burnup[1048] (referred to as 'evolution calculation'); it takes into account a large number of neutron energy groups (300 for typical calculations). It is mainly used to establish libraries of effective cross-sections[1049] which can then be used with the CRONOS software presented below; these are multiparameter libraries of effective sections (the parameters can be temperature, water density, etc.) condensed into a few energy groups and homogenized in the 'cells' chosen to represent the system

[1042] As indicated in Chapter 19 on reactor startup tests, it is not possible to cause accident situations to simply to ensure that equipment designed to control accident situations operates correctly.

[1043] See Neutronics, a monograph written by the CEA Nuclear Energy Division, published by *Éditions Le Moniteur*, 2013.

[1044] Simulation tools used in emergency situations are covered in Chapter 38.

[1045] Or their subcontractors.

[1046] A certain number of works are presented in the book entitled Current State of Research on Pressurized Water Reactor Safety by J. Couturier & M. Schwarz, Science and Technology Series, IRSN/EDP Sciences, 2017, as well as the book Nuclear Power Reactor Core Melt Accidents by D. Jacquemain et al., Science and Technology Series, IRSN/EDP Sciences, 2013.

[1047] In neutronics, a distinction is made between the expressions 'software' and 'computational scheme': 'computational scheme' refers to the sequence of physical models associated with a clearly defined library of effective cross-sections.

[1048] Fuel consumption through irradiation.

[1049] See Chapter 5, Section 5.2.

under study (assembly, rod, pellet, etc.). In principle[1050], APOLLO (2) can also be used to determine the core neutron balance (fission neutron production with respect to absorption and leakage) using the relevant neutron physics parameters (effective neutron multiplication factor *keff*, kinetic parameters – neutron lifetime or delayed neutron production – neutron feedback, absorber efficiency).

- **CRONOS:** this software for three-dimensional simulation of reactor core neutronics solves either the transport equation or the diffusion equation by using the finite element method for several neutron energy groups (two groups are sufficient for commonly used calculations). It is used to determine three-dimensional power distribution in the reactor core as well as the change in this power over time during incident or accident transients, the efficiency of neutron absorbers, etc. CRONOS software can also simulate fuel burnup (referred to as the 'evolution calculation'). The effective cross-sections necessary for computation come from results produced by APOLLO which are entered as input data in CRONOS, a code that can be used to simulate several plant series, since nothing in its organization or structure depends on the type of reactor. This means that computational schemes using CRONOS (2) have been built (notably in terms of meshing) for a large number of reactors (including research reactors).

- **MCNP**: this three-dimensional geometry simulation software, developed by the Los Alamos National Laboratory, was the first particle transport code based on the Monte Carlo method (Monte Carlo N-Particle transport code). MCNP software can be used for a variety of particles (neutrons, electrons, photons, etc.). It is used in several fields, including reactor physics, radiation protection, dosimetry, criticality and medical physics.

  For a reactor core, the principle consists in following the history of each neutron in the system under study, from birth (external source, fission neutron, etc.) to death (capture by a nucleus or escape from the system). With MCNP software, using a continuous neutron energy spectrum is usually chosen, but a discretized spectrum may also be used. Although MCNP software can simulate fuel burnup ('evolution calculation'), it is not suitable (similarly to the other Monte Carlo codes described below, at the current stage of their development) for simulating reactor transients, as neutron feedback does not correlate with temperature.

  The history of each neutron depends on its interaction with the material. The distance travelled by the neutron between two collisions, the nuclei involved and the interaction types are parameters that are randomly sampled using experiment results grouped into 'libraries' of nuclear data. In this way, by monitoring many neutrons, it is possible to simulate the natural behaviour of the system and calculate approximate numerical values of certain core neutron

[1050] This calculation is very complex with APOLLO (2); it became easier with APOLLO (3).

parameters (such as *keff* or kinetic coefficients, but not feedback, which depends on temperature). As this type of calculation is based on probabilities, extensive random sorting must be performed to reduce statistical uncertainty[1051]. Computation can sometimes last several months, hence the importance of using powerful computers. The geometrical representation of the system under study is based on a precise geometrical description of the surface of objects ('surface representation'), defined according to the problem to be dealt with; these objects can be of very different sizes (ranging from the area of a reactor core to a fuel pellet, for example). MCNP software can therefore be used for precise computation in neutronics.

– **TRIPOLI** (TRIdimensional POLYkinetics): this three-dimensional simulation software, under development by CEA since the 1960s, uses the Monte Carlo method to solve the transport equation for neutrons and photons, the latter resulting from the nuclear reactions generated by the neutrons (fission or capture - with photons leading to gamma radiation). In the same manner as MCNP software, using a continuous neutron energy spectrum is usually chosen for TRIPOLI, but a discretized spectrum may also be used. TRIPOLI software can simulate fuel burnup ('evolution calculation'), but, for the same reason as MCNP software, it cannot simulate reactor transients. With TRIPOLI, the system under study can be processed using surface definition (as for MCNP) or a combinatorial volume method (in which the user specifies the types of volume and the link between volumes). It is mainly used for reactor core physics, criticality and radiation protection. TRIPOLI is frequently used in France for precise calculations in neutronics (to calculate 'standards').

– **MORET:** this simulation software, developed since the 1970s, first by Professor Moret and then by IRSN, uses the Monte Carlo method to calculate neutron transport. It is generally used with a discretized neutron energy spectrum. The geometric representation is less detailed than representations achieved using the meshing tools associated with MCNP and TRIPOLI. MORET is used for complex three-dimensional systems containing fissile materials to determine the values of the following main parameters (excluding feedback correlated with temperature): the effective neutron multiplication factor (*keff*), neutron flux, reaction rates (fission, absorption and diffusion) in the different volumes, neutron escape from the system and kinetic system parameters (proportion of delayed neutrons and their generation time, neutron lifetime, etc.). The geometric model of the system under study is processed using the combinatorial volume method. More specifically, the software is used to study criticality risks in nuclear facilities (i.e. the occurrence of an uncontrolled chain reaction outside the reactor cores in operation), and operates within an 'environment'

[1051] The statistical uncertainty of a computation result is given by the central limit theorem: the standard deviation of the result is proportional to the inverse of the square root of the number of neutrons simulated.

known as CRISTAL[1052], which offers different datasets (and other codes such as APOLLO (2) and TRIPOLI (4)).

40.2. Simulation software for thermal hydraulics (and mechanics)

– **CATHARE** (an advanced thermal-hydraulic code for pressurized water reactor accidents): this two-phase thermal-hydraulic 'system code[1053]' has mainly been developed and used for safety analyses on pressurized water reactors (to study reactor thermal-hydraulic behaviour during incident or accident transients and develop the associated procedures), as well as for research and development work.

  CATHARE, developed jointly by CEA, EDF, Framatome and IRSN, has been operating and evolving since 1979. The core and systems selected for a study can be modelled in one dimension (1D), with the core represented by an 'average' channel or assembly; CATHARE also features a 3D module that can provide a three-dimensional representation of the vessel and core.

  CATHARE models the behaviour of the nuclear steam supply system of a pressurized water reactor from normal conditions up to the limits of the conventional design-basis conditions, i.e. up to the point where fuel is damaged.

  Finally, in order to train the teams that could be involved in an emergency situation, it was necessary to have tools capable of simulating the behaviour of the nuclear steam supply system. The SIPA simulator was developed by IPSN in the 1990s using CATHARE modules. It has since been replaced by the **SOFIA** simulator[1054], co-developed by Areva-NP (now Framatome) and IRSN. This simulator is used by IRSN in various contexts, for example, to train experts, reconstitute incidents or accidents, prepare accident scenarios for national emergency response exercises or others.

[1052] The CRISTAL criticality-safety package was developed and qualified as part of a collaborative project between IRSN, CEA, Areva NC (now Orano Cycle) and Areva-NP (now Framatome). This suite includes nuclear data libraries, computation procedures, simulation software and interface tools. Its purpose is to evaluate the criticality conditions of nuclear facilities and fissile material transport packaging.

[1053] A 'system code' is used to model an entire plant system and its components (fuel, exchangers, pumps, structures, etc.).

[1054] SOFIA (a simulator for observing operation during incidents and accidents) is an information system used by IRSN for studies and training. It can calculate and monitor changes in the physical parameters of a pressurized water reactor in real time. It simulates equipment failures and operator actions; computation can be stopped at any given moment to examine the state of the facility and it is possible to return to a previous point to change the scenario. The reactors modelled in SOFIA are those belonging to the French nuclear power fleet (900 MWe, 1300 MWe, 1450 MWe and EPR reactors).

- **FLICA:** developed by CEA beginning in 1967, this software simulates thermal hydraulics in a reactor core and the thermal properties of fuel. It has been used for several decades in reactors operating in France, including research reactors. FLICA (4) can be used to create a three-dimensional representation of a reactor core and to process the two phases of the coolant (liquid and steam). For thermal transfers in fuel, modelling is one-dimensional (1D).
- **HEMERA** (Highly Evolutionary Methods for Extensive Reactor Analyses) computer code: associated with CRONOS, FLICA can be used to obtain a more refined (3D) representation of the core for transient studies performed using the CATHARE system code. Figure 40.1 shows the coupling function available in the HEMERA computer code package used by IRSN and developed in cooperation with CEA.

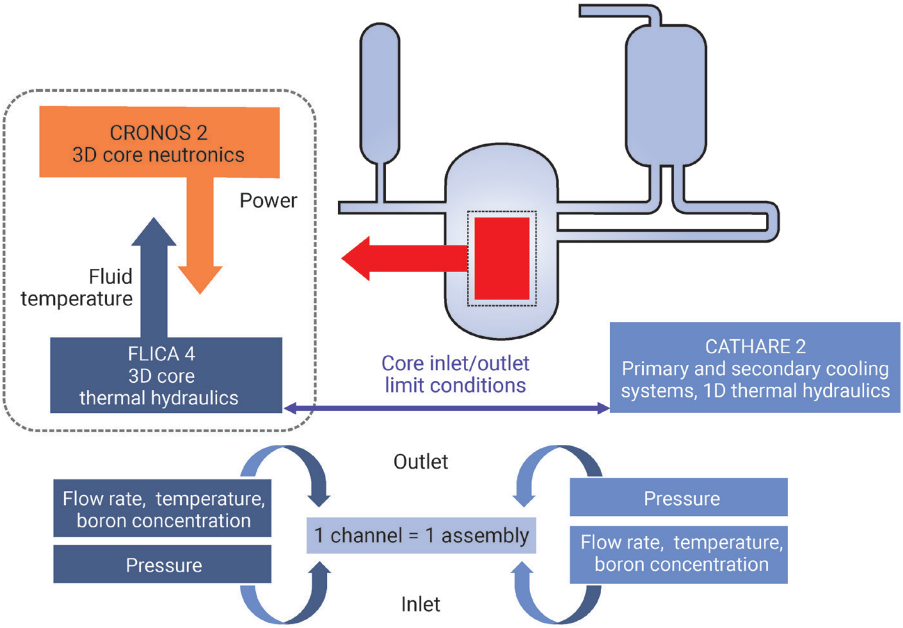


Figure 40.1. Coupling of CRONOS (2), FLICA (4) and CATHARE (2) (in the HEMERA software package) and the parameters interconnecting the three tools. IRSN.

The HEMERA software package is particularly suited for studying situations in which there is a strong coupling between neutron and thermal-hydraulic phenomena, such as ejection of a rod cluster control assembly or excessive core cooling, for example in the case of a steam-line break (SLB – see the computation example in Figure 40.2).

An explicit coupling technique has been adopted, where neutron and thermal-hydraulic equations are solved independently. Coupling is achieved through data transfer at the interfaces between the codes. This technique does require, however, performing some iterations outside the codes so that they converge correctly. A dedicated software tool (ISAS) is used to control the computer codes and check data exchanges.

Cross-sections are calculated using APOLLO (2), which generates a library referred to as 'multiparameter' because it can tabulate cross-sections according to the main operating parameters in a reactor (such as fuel burnup, temperature, coolant-moderator density, etc.). In the case of a reactivity accident, the effective cross-sections in particular are very sensitive to the burnup rate, temperature and moderator density. In the case of a steam-line break, the parameters of the effective cross-sections are added as a function of moderator temperature and boron concentration. This cross-section library is then used as input data for CRONOS (2).

Three-dimensional computation of reactor core neutronics and thermal hydraulics is performed using CRONOS (2) and FLICA (4), respectively. The approach adopted to model the core is based on an assembly-scale description (homogeneous modelling) since, in terms of computing time and memory capacity requirements, it is currently unfeasible to simulate the entire core with one simulation mesh per fuel rod (heterogeneous modelling). However, to obtain local information (at the fuel rod level) that could be necessary for the safety demonstration, HEMERA can focus on an assembly by modelling hybrid neutronics and thermal hydraulics[1055].

With CATHARE (2), each loop of the reactor coolant system is represented and modelling is one dimensional. For a 1300 MWe reactor, for example, about 600 meshes are defined.

The data calculated by CATHARE (2) and sent to FLICA (4) are:

- flow rate and enthalpy values at the core inlet,
- boron concentration values at the core inlet,
- profile of pressure values at the core outlet.

The data calculated by FLICA (4) and sent to CATHARE (2) are:

- flow rate and enthalpy values at the core outlet,
- boron concentration values at the core outlet,
- pressure profile at the core inlet.

[1055] 'Hybrid' modelling consists of performing a neutron calculation using CRONOS (2) rod by rod on a single assembly and one fourth of an assembly on the rest of the core, as well as a double thermal-hydraulic calculation using FLICA (4): a standard calculation for the entire core, where one assembly constitutes a channel, and one rod constitutes a channel only for a selected assembly. The boundary conditions for this assembly are given by the standard calculation. The advantage of hybrid modelling is the ability to calculate neutron feedback for each individual rod and thus obtain a rod-by-rod power distribution in a selected assembly (for example, an assembly that has undergone a power spike).

While CATHARE (2) provides data per reactor coolant loop, FLICA (4) needs these data for each fuel assembly. As a result, the data sent by CATHARE (2) are transformed by means of matrix processing, using a 'mix matrix' (where experiment coefficients quantify the various mixes in a pressurized water reactor vessel, divided into four quadrants), in order to obtain the surfaces representing the core inlet temperatures, flow rates and boron concentrations required for FLICA (4). Similar processing is carried out when data is sent from FLICA (4) to CATHARE (2).

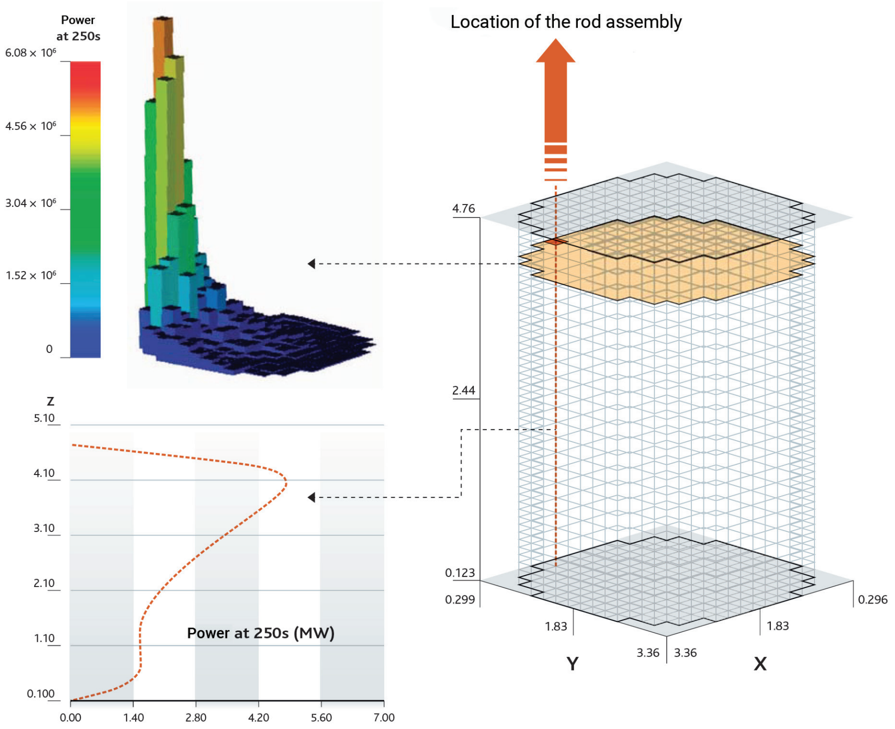


Figure 40.2. Example of application of the HEMERA software package: deformation of the power surface in the core in the event of a steam-line break (SLB) occurring while the reactor is shut down, assuming a rod cluster control assembly is jammed in the high position (aggravating event). IRSN.

It should be noted that IRSN primarily uses HEMERA for sensitivity studies of accident scenarios submitted by EDF. It is true that the approach commonly used in France for safety demonstrations is conservative, in other words, analyses will incorporate aggravating events into calculations used to simulate an accident situation, as well as conservatisms likely to amplify the consequences of the accident. For example, in the case of RCCA ejection (which causes a rapid rise in core power), this leads to increasing the reactivity insertion caused by RCCA ejection, while reducing the Doppler effect feedback. Since, in general, the goal is to limit the effects of neutron feedback, HEMERA has a certain number of 'neutron levers' to manipulate a large number of physical parameters as necessary and thus 'control' the accident kinetics. The most important parameters include, for example, changing reactivity insertion due to assembly ejection (for example, by choosing the assembly with the highest negative reactivity [or neutron weight]), changing the fraction of delayed neutrons and changing Doppler effects and the moderator.

- **DRACCAR** (code for studying deformation and reflooding of a fuel rod assembly during a cooling accident): this software, developed by IRSN, is a three-dimensional, multi-rod simulation tool that models the thermochemical and mechanical behaviour of water-cooled fuel rods, in particular to assess the maximum cladding temperature reached during a loss-of-coolant accident, to evaluate the blockage rate resulting from deformed rods and its impact on core cooling. This multiphysics software couples thermal phenomena (such as radiation), mechanical (such as cladding creep and rupture), thermochemical (such as cladding oxidation) and thermal-hydraulic phenomena that occur during a loss-of-coolant accident.

  To simulate thermal-hydraulic phenomena, DRACCAR couples two thermal-hydraulic computer codes that can be used to represent flows respectively within core channels and system channels:

  - CESAR, a thermal-hydraulics module developed by IRSN which is part of the ASTEC core-melt accident simulation software (see below),
  - CATHARE (3), presented above.

  DRACCAR is also used to simulate uncovery of fuel assemblies in the event of a loss-of-coolant accident that could affect a spent fuel storage pool.

  Material meltdown that may occur after rod cooling has been lost is outside the scope of simulation in DRACCAR.

- **Computational Fluid Dynamics (CFD) software**: this type of simulation software is used increasingly to determine local fluid flows by solving Navier-Stokes equations averaged over time and space and over a domain discretized by meshes with dimensions ranging from millimetres to centimetres.

  CFD software includes TrioCFD (formerly Trio-U), developed by CEA, STAR-CD® developed by Siemens and used by Areva and then Framatome, NEPTUNE_CFD developed by EDF, and CFX, developed by ANSYS and used by IRSN for its assessments.

  This type of software is suitable for studying scenarios of heterogeneous boron dilution in the reactor coolant system or asymmetric cold shock inside a pressurized water reactor vessel, which require fine modelling (from a few to about ten million meshes) of the thermal-hydraulic phenomena in the vessel.

Demonstration of the vessel fitness-for-service includes, among other things[1056], the study of cold-shock scenarios, which would result in a risk of sudden rupture under pressure. The penalizing scenarios considered are breaks (of a few inches in equivalent diameter) occurring in a reactor coolant loop, resulting in a safety injection of borated water, assumed at a temperature of 9°C, into a loop at 285°C. Figure 40.3 below shows how this type of scenario is modelled by IRSN using CFX software and gives an example of temperature distribution in the vessel during the transient. Sensitivity studies on various parameters (equivalent diameter of the break, safety injection flow rate, etc.) identify those which have the greatest influence on loads applied to the vessel, the extent of mixing phenomena in the loop where the safety injection occurs and in the vessel (annular downcomer, lower plenum, etc.).

It should be noted that the phenomenology of these scenarios is particularly complex. To ensure the predictive capability of CFD software, experimental programmes are conducted[1057].

40.3. Simulation software for thermal mechanics

- **SCANAIR:** this software, under development by IRSN since 1990, can be used to simulate the thermal-mechanical behaviour of fuel rods in pressurized water reactors during power transients, and to assess the risks associated with a loss of integrity or cladding failure. It is used in safety demonstrations and their analysis, and in defining, preparing and interpreting fuel rod performance tests during such transients (such as those conducted as part of the CABRI International Programme in the CABRI reactor). SCANAIR can simulate rapid reactivity insertion (Reactivity Injection Accidents – RIA) or slow power ramps such as those that could result from a steam-line break or even the uncontrolled withdrawal of a rod cluster control assembly in the core of a pressurized water reactor. In particular, SCANAIR models thermal-mechanical interaction between fuel pellets (UO_2, $UPuO_2$) and rod cladding, coolant boiling and the various cladding material deformation mechanisms.

[1056] Preventing the risk of sudden vessel rupture is based on periodic inspections, tests that anticipate changes in crack resistance in the relevant materials – under the effect of irradiation, which weakens them – and the study of accident scenarios such as the one described here, in order to verify that the requirements regarding the sudden rupture safety coefficients are met.

[1057] An example is the interlaboratory comparison conducted mainly between CFX and NEPTUNE_CFD software, based on experiments in the TOPFLOW-PTS facility in Germany (Helmholtz-Zentrum Dresden-Rossendorf – HZDR); the experiments were funded by the EU Commission (Framework Programme 7, 2007-2013), CEA, EDF, Areva NP, IRSN, the Paul Scherrer Institute and ETH in Zurich, Switzerland, and Helmholtz-Zentrum Dresden-Rossendorf.

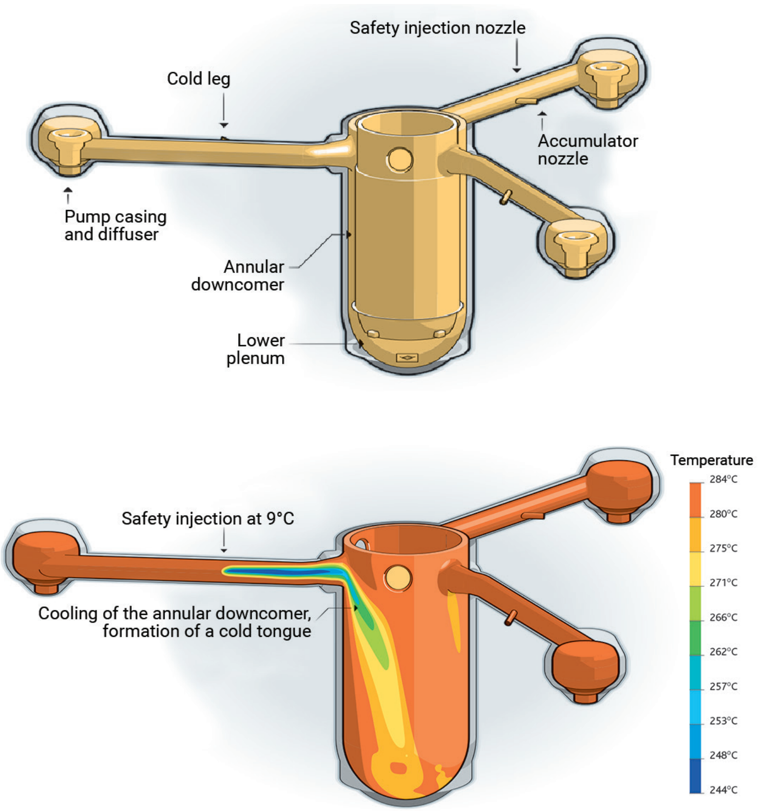


Figure 40.3. Study of a cold shock on a 900 MWe PWR vessel (IRSN). At the top, a model produced using CFX software, and at the bottom, visualization of the 'cold tongue' on the vessel (the top diagram is rotated by -120° with respect to the bottom one). IRSN.

40.4. Software for simulating core-melt situations

- **MC3D**: this is a multiphase thermal-hydraulic software package initially built by CEA and now developed by IRSN. It can be used to simulate the steam explosion that would result from a thermodynamic interaction between molten corium and reactor coolant, the type of phenomenon that could occur during a reactor core-melt accident. In particular, this software can be used to determine the dynamic pressure forces applied to structures (such as the walls of the reactor pool). It begins by simulating the first phase of the thermodynamic interaction, called 'pre-mixing', consisting of a coarse mixture of the two fluids, accompanied by more or less strong vaporization; under certain conditions, pre-mixing may be destabilized, which can lead to a violent explosion resembling a detonation (second phase).

- **ASTEC**: the Accident Source Term Evaluation Code simulation software aims to simulate all phenomena that would occur during a reactor core-melt accident, from the initiating event to any release of radioactive substances outside the reactor containment, with the exception of a steam explosion (which can be processed using MC3D) and the loads applied to structures (which can be processed using software such as Cast3M, see below). IPSN and later IRSN, together with their German counterpart GRS, developed ASTEC over a period of several years on the basis of the French ESCADRE system and German RALOC and FIPLOC software for containment thermal hydraulics; since 2017, only IRSN has pursued the development of ASTEC. ASTEC is mainly applied to safety analyses for pressurized water reactors, along with assessment of radioactive releases that could result from core melt in this type of reactor, and review of the operations that are or could be considered should this type of accident occur. ASTEC is also used by IRSN for its Level 2 probabilistic safety assessments. Lastly, it has also served in the preparation and interpretation of experimental programmes, in particular the Phébus-FP integral test programme and in tests carried out as part of the International Source Term Programme (ISTP).

  ASTEC and its later versions were applied in studies on the core-melt accident at TMI-2. It may also be noted that, with a view to dismantling the reactors at the Fukushima-Daiichi site, the Japanese government called on the services of the OECD/NEA as early as 2011 to better characterize, through simulation, the state of the three damaged reactors as well as the location of fuel debris. With this in mind, the BSAF project[1058] was created in 2011 to analyse progression of the accident during the first six days (and afterwards), using a database developed by the Japanese. Interlaboratory comparisons of the results obtained using various software packages, including ASTEC, MAAP developed by EPRI and MELCOR developed by Sandia Laboratories for the U.S. NRC, were conducted and when discrepancies were found, researchers searched for the causes. In addition to these analyses, models were recalibrated to adjust calculated releases to real-life measurements, using a ‘reverse analysis’ method to rebuild the amplitude and kinetics of releases on the basis of readings taken in the environment and calculated atmospheric dispersion.

  ASTEC is built according to a modular structure (see Figure 40.4), where each module simulates an area in the reactor or a subset of physical phenomena. The various ASTEC modules are shown below for a typical sequence of events during a reactor core-melt accident:

  - the ‘initial sequence’ phase (CESAR module) starts from the initiating event, such as a break in the reactor coolant system. Two-phase coolant flows develop in the system loops. All the reactor coolant is lost in the containment;

[1058] Benchmark Study of the Accident at the Fukushima-Daiichi Nuclear Power Station.

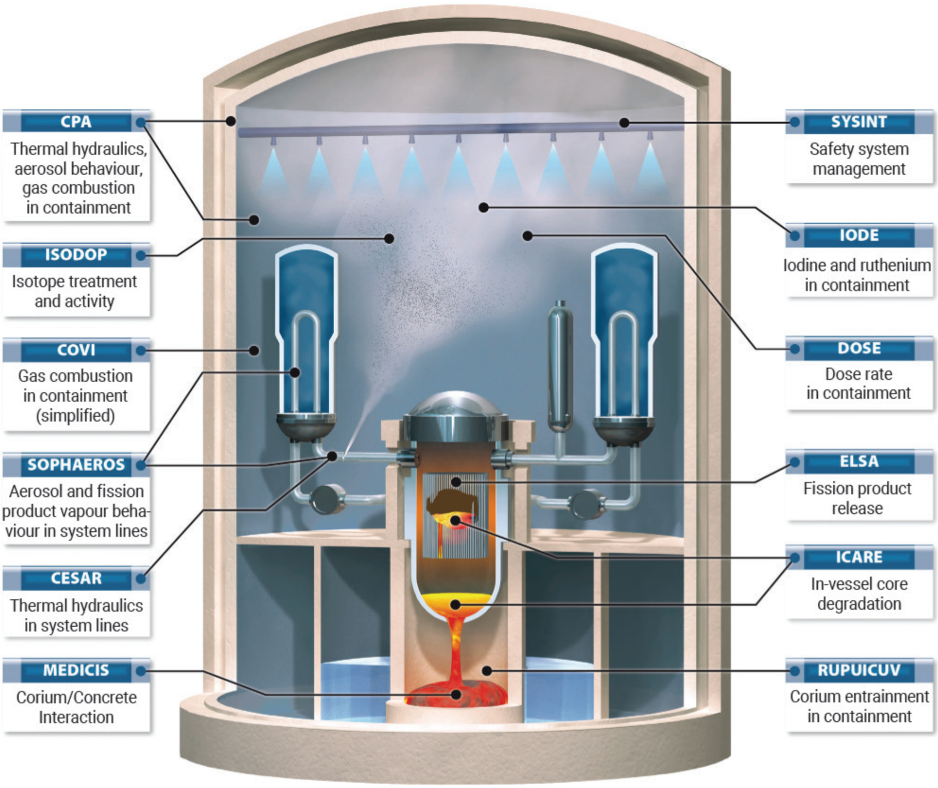

CPA
Thermal hydraulics, aerosol behaviour, gas combustion in containment
ISODOP
Isotope treatment and activity
COVI
Gas combustion in containment (simplified)
SOPHAEROS
Aerosol and fission product vapour behaviour in system lines
CESAR
Thermal hydraulics in system lines
MEDICIS
Corium/Concrete Interaction
SYSINT
Safety system management
IODE
Iodine and ruthenium in containment
DOSE
Dose rate in containment
ELSA
Fission product release
ICARE
In-vessel core degradation
RUPUICUV
Corium entrainment in containment

Figure 40.4. The various phenomena that occurred during a reactor core-melt accident and the modules simulating them in ASTEC. IRSN.

- the core heats up due to problems in removal of decay heat and the water level in the vessel decreases. Core degradation (ICARE module): there is exothermic oxidation of the zirconium alloy fuel rod cladding, caused by steam and the associated production of hydrogen; molten materials (corium) begin to mix at high temperature (up to 3000°C), then flow through the core and may relocate in the lower vessel plenum; an accumulation of corium heats the bottom of the vessel until it melts, leading to a mechanical breach;
- fission products (FP) are released from damaged fuel rods (ELSA module): initially, they are fission gases and more volatile products such as iodine and caesium, followed by less volatile fission products such as molybdenum after more severe rod degradation. Materials from structures, including rod cluster control assemblies and grids, are also released as vapour;

- the aerosols formed and fission product vapours are transported by the vapour flow into the reactor coolant system (SOPHAEROS module) and reach the containment. They can form deposits and be resuspended later. Species can vary according to chemical interactions, especially in the gaseous phase;
- after the bottom of the vessel has ruptured, corium flows into the reactor pit due to the reactor coolant system pressure. A certain fraction of the corium at high temperature may enter the containment, contributing to the temperature rise inside (DCH phase[1059]) (RUPUICUV module);
- the corium remaining in the reactor pit interacts with the concrete of the basemat (MCCI phase[1060]) (MEDICIS module), leading to ablation of the concrete layer and release of non-condensable gases (H_2, CO, CO_2, etc.) in the containment;
- the containment atmosphere is heated through the combined effect of water vapour sources, fission products and aerosols (CPA module), and pressure rises. Combustion of accumulated hydrogen can occur and induce dynamic loading forces inside the containment;
- the behaviour of iodine in the containment is an important subject (SOPHAEROS module), since iodine has a particularly important role in terms of short-term radiological consequences; its chemical behaviour and the effect of radiation largely determine the radiological impact; this element adsorbs and desorbs on the walls of the containment (especially on painted surfaces) and its chemical and physical state evolves in the aqueous and gaseous phases[1061].

Other modules describe the progression and transfer of decay heat, as well as fission product activity in the containment (ISODOP module), and the impact of safety systems on the sequence of events during the accident, for example when the containment water spraying system or the safety injection accumulators are set into action (SYSINT module).

40.5. Simulation software for mechanics

– **Cast3M**: this finite element simulation software was developed by CEA for structural and fluid mechanics. It is widely used by designers and operators of French nuclear facilities for applications related to metal structures or civil works (pools, reactor buildings, etc.), particularly pressurized water reactors in the French nuclear power plant fleet. It is also widely used by IRSN, which at times may need to request specific development services from CEA. For example, in the field of civil engineering, developments include finding laws

[1059] Direct containment heating.

[1060] Corium-concrete interaction.

[1061] SOPHAEROS processes iodine chemistry in the reactor coolant system.

to simulate delayed or dynamic behaviour of concrete structures subjected to loading forces in an accident situation (such as an earthquake). These developments are then integrated into Cast3M to make them available to all Cast3M users. Figure 40.5 shows an example of how it is used.

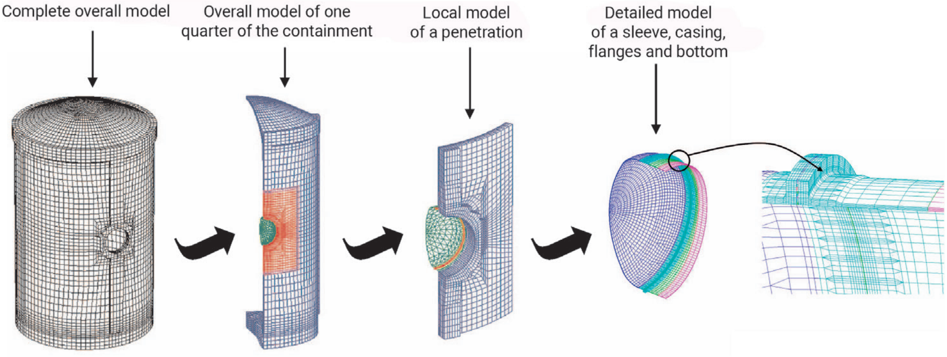

Complete overall model
Overall model of one quarter of the containment
Local model of a penetration
Detailed model of a sleeve, casing, flanges and bottom

Figure 40.5. IRSN modelling using Cast3M to represent a pressurized water reactor containment and the equipment hatch area. Georges Nahas/IRSN.

- **EUROPLEXUS, LS-DYNA:** EUROPLEXUS software uses finite element simulation to represent fast dynamic phenomena, taking into account structures and fluids, originally developed by CEA (PLEXUS code) and the Joint Research Centre in Ispra, Italy (PLEXUS-3C), and later taken over by a group of users including EDF and ONERA. LS-DYNA is a similar type of computer code developed by Livermore Software Technology Corporation (LSTC) in the USA. These codes can be used to study the behaviour of structures subjected to shocks, for example.

40.6. Fire simulation software

- **SYLVIA**: IRSN has been developing SYLVIA (a software system used to study fire, ventilation and airborne contamination) since the early 2000s to simulate the progression and consequences of a fire in an industrial facility equipped with a ventilation system, focusing on development of the fire, transport of hot gases and soot, and re-suspension and transport of aerosols. It can estimate filter clogging and possible damage to compartmentation equipment such as fire doors and fire dampers.

  In the model, the space in each room is divided into two zones of variable height in which the thermodynamic properties (pressure, temperature and concentration of gaseous and particulate species) are uniform, with the upper zone containing hot gases and fumes. The complete ventilation system is modelled with all its equipment, including ducts, filters, dampers, fans, etc. Correlations of the mass and heat exchange between the zones, flames and walls complete the mass and energy balance equations for the zones under study. Combustion models for complex solid fires (such as glove boxes, electrical cabinets, electrical cable trays, waste drums, etc.) are available and are gradually being improved. Rates of aerosol resuspension and deposition on the walls of rooms and in the ventilation system are also estimated.

SYLVIA can process all the above phenomena with full coupling and different levels of modelling from a simple room to a complete nuclear facility, including its entire ventilation system.

SYLVIA is IRSN's reference tool for calculating fire risk and is used for IRSN safety assessments of nuclear facilities. With high-performance computing capability (low calculation time), it can carry out hundreds of simulations for probabilistic safety studies on fire risk for reactors in the French nuclear power plant fleet. Coupled with the SUNSET[1062] statistical tool developed by IRSN, SYLVIA is used to produce exhaustive parameter studies and to analyse the sensitivity of results to parameters of interest.

– **ISIS**: the ISIS software package developed by IRSN since the mid-2000s provides a three-dimensional simulation of weakly compressible, turbulent and reactive flows. It offers a coherent set of models for flow turbulence, combustion, soot production and heat transfer to describe fire development in large compartments that are either naturally ventilated, or confined and mechanically ventilated. ISIS has been validated in a series of analytical and comprehensive tests.

  Coupling ISIS with SYLVIA combines the accuracy of the ISIS 3-D simulator to assess the consequences of a fire in a room and the computing power of SYLVIA to describe an entire ventilation system.

– **P^{2}REMICS**: a software package for numerical simulation of explosions in industrial facilities; it can be used to calculate the formation of an explosive atmosphere (including mixtures of hydrogen and air, or suspension of fine dust), its deflagration and propagation of the resulting blast waves.

  First developed in 2013, P^{2}REMICS is used to simulate flows, including three-dimensional, incompressible (explosive atmosphere formation phase) or compressible (deflagration and shock-wave propagation), turbulent and reactive flows. Turbulence can be processed using different models. To process deflagration in large rooms, P^{2}REMICS includes an explicit flame-front tracking model, which requires lower resolution discretization of space than for solving primitive conservation equations in reactive fluid mechanics. The latter are preferably used to build flame velocity databases for a mixture of gases, which will then serve as input data for full-scale simulations (in a multi-scale approach).

  IRSN has developed P^{2}REMICS in cooperation with outside partners (INERIS and the ICARE Institute), primarily French universities and CNRS laboratories. It thus benefits from strong scientific support in modelling of turbulence, gas and dust combustion and numerical analysis.

[1062] Sensitivity and Uncertainty Statistical Evaluation Tool.

The safety issues addressed to date using P^{2}REMICS are essentially hydrogen explosions, either in the containment of a pressurized water reactor in loss-of-coolant or core-melt accident situations, or the loss of integrity on hydrogen tanks and piping inside and outside the reactor building. P^{2}REMICS is also suitable for studying gas and dust mixtures such as those that would occur, for example, in the event of a loss of vacuum in the ITER torus.

Videos available for viewing

DRACCAR
Simulation Code

ASTEC
Simulation Software (in French)

ISIS
Simulation Code (in French)

List of Acronyms

Acronyms for institutions, bodies and groups

ACRO: French Association for the Control of Radioactivity in the West (*Association pour le contrôle de la radioactivité dans l'Ouest*)

ACRS: Advisory Committee on Reactor Safeguards (U.S. NRC support body)

AEC: Atomic Energy Commission (superseded by the U.S. Nuclear Regulatory Commission in 1974)

AERES: French Agency for the Evaluation of Research and Higher Education (*Agence d'évaluation de la recherche et de l'enseignement supérieur*), replaced by HCERES

AFCEN: French Association for Rules on the Design, Construction and In-service Inspection of Components Used in Industrial or Experimental Nuclear Power Facilities (*Association française pour les règles de conception, de construction et de surveillance en exploitation des matériels des chaudières électronucléaires*)

AFCN: Belgian Federal Agency for Nuclear Control (*Federaal Agentschap voor Nucleaire Controle*)

AFFSE: French Agency for Safety in Health and Environmental Affairs (*Agence française de sécurité sanitaire et environnementale*) replaced by ANSES

AIB-Vinçotte: an accredited inspection and certification company in the field of safety and reliability in Belgium (*Association des industriels de Belgique-Vinçotte*)

ANCCLI: French National Association of Local Information Commissions (*Association nationale des comités et commissions locales d'information*)

ANCLI: French national association of local information commissions (*Association nationale des commissions locales d'information*)

ANDRA: French National Radioactive Waste Management Agency (*Agence nationale pour la gestion des déchets radioactifs*)

ANR: French National Research Agency (*Agence nationale de la recherche*)

ANS: American Nuclear Society

ANSI: American National Standards Institute

ANSYS (ANSYS, Inc.): US simulation software publisher

APAVE: French Association of Owners of Steam and Electrical Appliances (*Association de propriétaires d'appareils à vapeur et électriques*)

APEL: Loire Valley Environmental Action Organization (*Action pilote environnement Loire, France*)

Areva: French nuclear designer and operator. Company created in 2001 by the merger between Framatome (which later became Areva NP) and Cogéma (which later became Areva NC), then restructured in 2018 to create Framatome, the nuclear power reactor designer – a subsidiary of the EDF Group – and Orano for the fuel cycle, including the development of reactor fuel assembly components

ASCOT: Assessment of Safety Culture in Organizations Team

ASME: American Society of Mechanical Engineers. The acronym is often used to refer to the design and construction rules established by this US professional society, which serve as a reference for nuclear reactor designers (Westinghouse, etc.)

ASN: French Nuclear Safety Authority (*Autorité de sûreté nucléaire*)

ASSET: Assessment of Safety Significant Event Team (IAEA)

AVN: Association Vinçotte-Nuclear, Belgium

Babcock & Wilcox: US nuclear power reactor designer

BCCN: French Inspectorate of Nuclear Steam Supply Systems, superseded by ASN/DEP (*Bureau de contrôle des chaudières nucléaires*)

Bel V: Belgian federal nuclear control agency, created as a subsidiary of AFCN. As an expert in nuclear safety since 2008, Bel V has taken over the regulatory inspections previously carried out by AVN in power plants and other nuclear and radiological facilities in Belgium

BMU: German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (*Bundesministerium für Umwelt, Naturschutz und Reactorsicherheit*)

BNRA: Bulgarian Nuclear Regulatory Agency

BRGM: French Geological Survey (*Bureau de recherches géologiques et minières*)

CEA: French Alternative Energies and Atomic Energy Commission (*Commissariat à l'énergie atomique,* now *Commissariat à l'énergie atomique et aux énergies alternatives*)

CEPN: French Nuclear Protection Assessment Centre (*Centre d'étude sur l'évaluation de la protection dans le domaine nucléaire*)

CFDT: labour union, the French Democratic Confederation of Labour (*Confédération française démocratique du travail*)

CHSCT: health, safety and working conditions committee, a structure required in corporations and institutions according to French labour laws (*Comité d'hygiène, de sécurité et des conditions de travail*)

CIC: Interministerial Emergency Response Unit (*Cellule interministérielle de crise*), France

CIEE: French Information Council on Nuclear Power Generation (*Conseil de l'information sur l'énergie électronucléaire*)

CIINB: French Interministerial Commission for Basic Nuclear Installations (*Commission interministérielle des installations nucléaires de base*)

CIREA: French Interministerial Commission on Artificial Radionuclides (*Commission interministérielle des radioéléments artificiels*)

CIS Bio International: company that develops, manufactures and markets radionuclides for nuclear diagnostics and radiotherapy, located in Gif-sur-Yvette, France

CLI: Local Information Commission (*Commission locale d'information*), France

CM: Mobil unit, part of IRSN's emergency response organisation (*Cellule mobile*)

CNPE: French acronym used by EDF for 'nuclear power plant' (*Centre nucléaire de production d'électricité*), France

CNRA: Committee on Nuclear Regulatory Activities (OECD/NEA)

CNRS: French National Centre for Scientific Research (*Centre national de la recherche scientifique*)

CODIRPA: French Steering Committee for Management of the Post-Accident Phase (of a nuclear accident or radiological emergency) (*Comité directeur pour la gestion de la phase post-accidentelle*)

COFSOH: French Steering Committee on Human, Social and Organizational Factors (*Comité d'orientation sur les facteurs sociaux, organisationnels et humains*)

Cogema: General Company for Nuclear Materials (subsequently AREVA NC, then Orano) (*Compagnie générale des matières nucléaires*)

COPAT: EDF Reactor Outage Operational Centre for the French nuclear power plant flet (*Centre opérationnel de pilotage d'un arrêt de réacteur du parc électronucléaire français*)

COS: Commander of prefecture emergency response operations (*Commandant des opérations de secours, en préfecture*), France

CRIIRAD: Commission for Independent Research and Information on Radioactivity (*Commission de recherche et d'information indépendantes sur la radioactivité*), France

CRPPH: Committee on Radiological Protection and Public Health (NEA)

CS: Healt unit, part of IRSN's emergency response organization (*Cellule "santé"*)

CSIA: committee for the security of atomic installations (now the Commission for the security of atomic installations) (*Comité de la sécurité des installations, now Commission de la sécurité des installations*)

CSNI: Committee on the Safety of Nuclear Installations, OECD/NEA

CSP: Atomic Pile Safety Commission, renamed CSR (*Commission de sûreté des piles*), France

CSPI : special permanent information commission (*Commission spéciale permanente d'information*)

CSPRT: High Council for the Prevention of Technological Risks (*Conseil supérieur de la prévention des risques technologiques*), France

CSR: Reactor Safety Commission, DSND (*Commission de sûreté des réacteurs*), France

CSS: Commission on Safety Standards, IAEA

CSSIN: French High Council for Nuclear Safety and Information (*Conseil supérieur de la sûreté et de l'information nucléaires*)

CSSN: High Council for Nuclear Safety (*Conseil supérieur de la sûreté nucléaire*), France

CTC: IRSN Emergency Response Centre (*Centre technique de crise*)

CVŘ (UJV Group): Nuclear Energy Research and Development Centre, Husinec-Řež, Czech Republic (*Centrum výzkumu Řež*)

DEP: Nuclear Pressure Equipment Department (*Direction des équipements sous pression*), ASN, France

DFD: Franco-German Management Committee (*Deutsche-Französischer Direktionausschuss*)

DFK: Franco-German Commission (*Deutsche-Französiche Kommission*)

DGEC: Directorate-General for Energy and Climate within the Ministry for Ecological and Inclusive Transition (*Direction générale de l'énergie et du climat du ministère en charge de la transition écologique et solidaire*), France

DGPR: Directorate-General for Risk Prevention (*Direction générale de la prévention des risques*), France

DGSNR: Directorate-General for Nuclear Safety and Radiation Protection (*Direction générale de la sûreté nucléaire et de la radioprotection*), France

DITEIM: Directorate for Technology, the Industrial Environment and Mines (*Direction de la technologie, de l'environnement industriel et des mines*), France

DoD: US Department of Defense

DOE: US Department of Energy

DPN: Nuclear Generation Division (*Direction de la production nucléaire*), EDF, France

DREAL: Regional Directorate for the Environment, Town and Country Planning and Housing (*Direction régionale de l'environnement, de l'aménagement et du logement*), Paris region, France

DRIEE: Regional and intermuniciple directorates for the environment and energy (*Directions régionales et interdépartementales de l'environnement et de l'énergie*)

DRIRE: Regional Industry, Research and Environment Directorate (*Direction régionale de l'industrie, de la recherche et de l'environnement*), France; (all DRIRE regional directorates have been replaced by DREAL directorates)

DSIN: Directorate for the Safety of Nuclear Installations (*Direction de la sûreté des installations nucléaires*), France

DSN: Nuclear Safety Department (*Département de sûreté nucléaire*), CEA, France

DSND: representative in charge of nuclear safety and radiological protection for French defence-related activities and facilities (*Délégué à la sûreté nucléaire et à la radioprotection pour les activités et installations intéressant la Défense*)

EBRD: European Bank for Reconstruction and Development

EDF: French electrical power utility (Électricité de France)

EFQM: European Foundation for Quality Management

EIB: European Investment Bank

ELC: local emergency response team at French nuclear facilities (*Équipe locale de crise*)

ENEA: Italian National Atomic Energy Agency, now the National Agency for New Technologies, Energy and Sustainable Economic Development (*Ente Nazionale Energia Atomica, now Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile*)

ENGIE Electrabel: Belgian corporation operating nuclear power reactors

ENSREG: European Nuclear Safety Regulators Group (European Commission advisory group of regulatory authority experts)

ENSTTI : European Nuclear Safety Training and Tutoring Institute (no longer exists)

ENUSA: a Spanish company founded in 1972 that designs, produces and distributes nuclear fuel for Spanish nuclear power plants and power plants in other country (*Empresa Nacional del Uranio SA*)

EPRI: Electric Power Research Institute (USA)

EPRUS: Organization for Public Health Emergency Preparedness and Response (*Établissement de préparation et de réponse aux urgences sanitaires*), France

ETC-N: EDF national emergency response technical team (*Équipe technique de crise au niveau national d'EDF*)

ETSON: European Technical Safety Organisations Network (TSO)

EU: European Union

Euratom: European Atomic Energy Community

EURELECTRIC: an association established in 1989 representing the common interests of the electricity industry at the European level, as well as its subsidiaries and associates on several other continents. EURELECTRIC covers all the major subjects of interest in this sector, from power generation and markets to distribution networks and customer issues

EUROSAFE: forum promoting nuclear safety in Europe

FANC: Federal Agency for Nuclear Control, Belgium

FARS: Fuel Assembly Repair Station; Areva equipment for extracting one or more rods from an AFA fuel assembly

FENOC: First Energy Nuclear Operating Corporation (US nuclear reactor operator)

Framatome: French designer of pressurized water reactors, subsequently incorporated into the Areva group as 'Areva NP'

FzK (formerly KIT): Karlsruhe Institute of Technology (Forschungszentrum Karlsruhe), Germany

GANIL: Major national heavy-ion accelerator research centre in Caen (*Grand accélérateur national d'ions lourds*), France

GPD: Advisory Committee for Waste (*Groupe permanent d'experts pour les déchets*), ASN, France

GPDEM: Advisory Committee for the Decommissioning of Nuclear Facilities (*Groupe permanent d'experts pour le démantèlement des installations nucléaires*), ASN, France

GPE: Advisory Committees (*Groupes permanents d'experts*), ASN, France

GPEC: Strategic workforce planning (*Gestion prévisionnelle des emplois et des compétences*)

GPESPN: Advisory Committee for Nuclear Pressure Equipment (*Groupe permanent d'experts pour les équipements sous pression nucléaires*), ASN, France

GPMED: Advisory Committee for Radiation Protection in the Medical Sector (*Groupe permanent d'experts pour la radioprotection dans les applications médicales*), ASN, France

GPR: Advisory Committee for Reactors (*Groupe permanent d'experts pour les réacteurs nucléaires*), ASN, France

GPRAD: Advisory Committee for Environment and Radiation Protection (*Groupe permanent d'experts pour la radioprotection dans les applications industrielles et de recherche des rayonnements ionisants et en environnement*), ASN, France

GPT: Advisory Committee for Transport (*Groupe permanent d'experts pour les transports*), ASN, France

GPU: Advisory Committee for Laboratories and Plants (*Groupe permanent d'experts pour les laboratoires et les usines*), ASN, France

GRNC: Nord-Cotentin Radioecology Group (*Groupe radioécologique Nord-Cotentin*), France

GRS: Safety Organization for Nuclear Reactors and Facilities (*Gesellschaft für Anlagen- und Reaktorsicherheit*), Germany

GSIEN: Scientific Group for Nuclear Energy Information (*Groupement de scientifiques pour l'information sur l'énergie nucléaire*), France

HAMMLAB: Halden Man-Machine Laboratory, Norway

HCERES: High Council for Evaluation of Research and Higher Education (*Haut conseil de l'évaluation de la recherche et de l'enseignement supérieur*) (replaced AERES), France

HCTISN: French High Committee for Transparency and Information on Nuclear Security, France (*Haut comité pour la transparence et l'information sur la sécurité nucléaire*)

HFDS: Senior Defence and Security Official (*Haut fonctionnaire de défense et de sécurité*) under the Ministry of Ecology, Sustainable Development and Energy, France

HSE: Health and Safety Executive (competent authority for labour inspection in the fields of health and safety at work, United Kingdom)

HZDR: Helmholtz-Zentrum Dresden-Rossendorf

IAEA: International Atomic Energy Agency, Vienna, Austria

ICARE: Institute for Combustion, Aerothermic, Reactivity and Environment (*Institut de combustion, aérothermique, réactivité et environnement*), France

ICRP: International Commission on Radiological Protection

IEC: International Electrotechnical Commission (publishes standards)

IEEE: Institute of Electrical and Electronics Engineers (professional association that publishes standards)

IEER: Institute for Energy and Environmental Research, USA

IFA: Franco-German initiative for Chernobyl, focused on thyroid cancer in children

IFSTTAR: French Institute of Science and Technology for Transport, Development and Networks (*Institut français des sciences et technologies des transports, de l'aménagement et des réseaux*)

ILL: Institut Laue-Langevin, Grenoble, France (operates the High Flux Reactor)

INERIS: French National Institute for the Study of Industrial Environments and Risks (*Institut national de l'environnement industriel et des risques*), France

INL: Idaho National Laboratory, USA

INPES: French National Institute for Education on Prevention and Education in Health Affairs (*Institut national de prévention et d'éducation pour la santé*)

INPO: Institute of Nuclear Power Operations, USA

INSAG: International Nuclear Safety Advisory Group (group of international experts in nuclear safety that advises the IAEA)

INSEE: French National Institute of Statistics and Economic Studies (*Institut national de la statistique et des études économiques*)

INSERM: French National Institute of Health and Medical Research (*Institut national de la santé et de la recherche médicale*), France

INTRA: economic interest group of French nuclear operators created after the Chernobyl accident whose goal is to develop robotic devices that can intervene in a highly radioactive environment

InVS: French National Institute for Public Health Surveillance (*Institut de veille sanitaire*)

IPSN (now IRSN): Institute for Protection and Nuclear Safety (*Institut de protection et de sûreté nucléaire*), France

IRRS: Integrated Regulatory Review Service, IAEA

IRRT: International Regulatory Review Team (former IRRS), an IAEA service

IRSN: Institute for Radiological Protection and Nuclear Safety (*Institut de radioprotection et de sûreté nucléaire*), France

ISO: International Organization for Standardization

ITER Organization: an intergovernmental organization (whose members include the People's Republic of China, the European Atomic Energy Community (Euratom), India, Japan, Korea, the Russian Federation and the USA), which seeks to demonstrate the scientific and technical feasibility of the peaceful uses of fusion energy

JAEA: Japan Atomic Energy Agency

JNES: Japan Nuclear Energy Safety Organization

JRC: Joint Research Centre, European Commission (with facilities in Petten, Netherlands, Ispra, Italy, and other locations)

JSI: Jožef Stefan Institute (research institute established in 1949, responsible for a broad spectrum of basic and applied research in the fields of natural sciences and technology, Ljubljana, Slovenia)

KEPCO: Kansai Electric Power Company, Japan

KTA: Kerntechnische Ausschuss (comité nucléaire allemand, par assimilation nom donné aux règles établies par ce comité)

KWU: German KONVOI reactor manufacturer (*Kraftwerk Union*)

LEI: Lithuanian Energy Institute (Kaunas, Lithuania)

LSTC: Livermore Software Technology Corporation, USA

MAI: Materials Ageing Institute (founded by EDF to study equipment ageing)

MEDDE: Ministry of Ecology, Sustainable Development and Energy (*Ministère de l'écologie, du développement durable et de l'énergie*), now the Ministry for Ecological and Inclusive Transition (MTES), France

METI: Ministry of Economy, Trade and Industry, Japan

MOE: Ministry of the Environment, Japan

MSNR: Nuclear Safety and Radiation Protection Mission (*Mission de sûreté nucléaire et de radioprotection*) in the Directorate-General for Risk Prevention of the Ministry for Ecological and Inclusive Transition, France

MSQ, MSQE: Quality Safety Team, now the Environmental Quality Safety Team (*Mission sûreté qualité, Mission sûreté qualité environnement*), an entity within EDF

MTA EK: Hungarian Academy of Sciences, Centre for Energy Research, Budapest

MTES: Ministry for Ecological and Inclusive Transition (*Ministère de la transition écologique et solidaire*), France

NDC: Nuclear Development Committee (committee for technical and economic studies on nuclear energy development and the fuel cycle, OECD/NEA)

NEA: Nuclear Energy Agency, operating within the OECD

NEI: Nuclear Energy Institute, USA

NHK: Japanese television channel

NISA: Nuclear and Industrial Safety Agency, Japan

NLC: Nuclear Law Committee, OECD/NEA

NPI: Nuclear Power International (subsidiary created by Framatome and Siemens)

NRA: Nuclear Regulation Authority (new Japanese nuclear regulatory authority, established after the accident at the Fukushima Daiichi nuclear power plant)

NSC: Nuclear Science Committee, OECD/NEA

NSC: Nuclear Safety Commission, Japan

NTTF: Near-Term Task Force set up in the USA following the accident at the Fukushima Daiichi nuclear power plant

NUGENIA: NUclear GENeration II & III Association (international association dedicated to safety on second- and third-generation reactors)

NuScale Power: US company that is developing a small integrated modular 50 MWe pressurized water reactor

NUSSC: NUclear Safety Standards Committee, IAEA

OECD: Organisation for Economic Co-operation and Development

OPECST: Parliamentary Office for the Evaluation of Scientific and Technological Options (*Office parlementaire d'évaluation des choix scientifiques et technologiques*), France

OPRI: Office for Protection against Ionizing Radiation (*Office de protection contre les rayonnements ionisants*), France

Orano: see Areva

ORNL: Oak Ridge National Laboratory, Tennessee, USA

OSART: Operational SAfety Review Team; safety assessment of a nuclear site, organized by the IAEA at the request of a Member State

PROSPER: Peer Review of Operational Safety Performance Experience Review, IAEA

PSI: Paul Scherrer Institute, Switzerland

RASSC: Radiation Safety Standards Committee, IAEA

RATEN ICN: Institute for Nuclear Research Pitesti (*Institutul de Cercetari Nucleare)*, Romania

RDM: a Dutch company that manufactured reactor vessels, but no longer exists (*Rotterdamsche Droogdokmaatschappij*)

RHWG: Reactor Harmonization Working Group (WENRA Working Group on Reactor Safety Harmonization)

RISKAUDIT: IRSN/GRS economic interest group (no longer exists)

ROSATOM: Russian company specializing in the design, construction and operation of power reactors

RSK: Reactor Safety Commission (*Reaktor-Sicherheitskommission*), Germany

RWMC: Radioactive Waste Management Committee, OECD/NEA

SAFER: Strategic Alliance for FLEX Emergency Response

Santé publique France: French state-owned administrative entity, under the supervision of the Minister of Health. Replaced the National Health Surveillance Institute (*Institut de veille sanitaire*, InVS), the National Institute for Prevention and Education in Health Affairs (*Institut national de prévention et d'éducation pour la santé*, INPES), and the Organization for Public Health Emergency Preparedness and Response (*Établissement de préparation et de réponse aux urgences sanitaires*, EPRUS)

SCPRI: Central Service for Protection against Ionizing Radiation (*Service central de protection contre les rayonnements ionisants*), France

SCSIN: Central Service for the Safety of Nuclear Installations (*Service central de sûreté des installations nucléaires*), France

SCSP: Subcommittee on Atomic Pile Safety (*Sous-commission de sûreté des piles*), France

SCSSINP: State Committee for the Supervision of Safety in Industry and Nuclear Power, USSR

SEBIM: manufacturer of valves for pressurized water reactors in the French nuclear power plant fleet

SEC NRS: Scientific and Engineering Centre for Nuclear and Radiation Safety, Moscow, Russian Federation

SGDSN: French General Secretariat for Defence and National Security (*Secrétariat général de la défense et de la sécurité nationale*), France

SPR: radiation protection department of CEA, now obsolete (*Service de protection contre les radiations*)

SSTC NRS: State Scientific and Technical Centre for Nuclear and Radiation Safety, Kiev, Ukraine

TEPCO: Tokyo Electric Power Company (operator of the reactors at the Fukushima Daiichi nuclear power plant in Japan)

TRANSSC: TRANsport Safety Standards Committee, IAEA

TSO: Technical Safety Organisation

UJV: see CV Řež

UNIPEDE: International Union of Producers and Distributors of Electrical Energy

UNSCEAR: United Nations Scientific Committee on the Effects of Atomic Radiation

U.S. NRC: US Nuclear Regulatory Commission

UTO: Corporate Technical Support Department (*Unité technique opérationnelle*), EDF/DPN

VATESI: State Nuclear Power Safety Inspectorate (Lithuanian safety authority)

VTT: Technical Research Centre of Finland (*Valtion Teknillinen Tutkimuskeskus*)

VUJE: engineering company established in 1977, active in design, supply, implementation, research and training mainly in the field of nuclear and conventional energy, Trnava, Slovakia

WANO: World Association of Nuclear Operators

WASSC: WAste Safety Standards Committee, IAEA

WENRA: Western European Nuclear Regulators Association

Westinghouse: American company founded by George Westinghouse in 1886 as Westinghouse Electric Company and acquired by the Japanese firm Toshiba in 2006. It specializes in the nuclear industry, including the design and manufacture of nuclear fuel assemblies, specialized services to industry and associated engineering, and the design and construction of new nuclear power plants

WGOE: Working Group on Operating Experience, OECD/NEA

WHO: World Health Organization

WISE-Paris: World Information Service on Energy (independent agency for information, study and advising on nuclear and energy policy)

Wood: Wood Environment & Infrastructure Solutions has joined forces with Amec Foster Wheeler to form an organization providing project, engineering and technical services to the energy and industrial markets, Knutsford, UK

Technical acronyms and abbreviations

AFA: generic name for fuel assemblies produced by Areva and later Framatome, which are loaded in French nuclear power reactors

AFIS: Westinghouse tool using ultrasound to locate leaking fuel rods in a fuel assembly

AFP: Auxiliary Feedwater Pump

AGORAS: research project on nuclear safety and radiation protection funded by the French National Research Agency to improve the governance of organizations and stakeholder networks for nuclear safety (*Amélioration de la gouvernance des organisations et des réseaux d'acteurs pour la sûreté nucléaire*)

AIC: a mixture of silver, indium and cadmium used as a neutron-absorbing material in pressurized water reactors

ALARA: As Low As Reasonably Achievable; a principle used in particular in radiation protection

ALCADE: campaign to improve operations by managing fuel for reactors in the French nuclear power plant fleet (*Allonger les campagnes pour améliorer durablement l'exploitation*)

ALPS: Advanced Liquid Processing System; system developed by the operator TEPCO to treat contaminated water recovered after the accident at the Fukushima Daiichi Nuclear Power Plant

AMS: Aeroball Measuring System; name of the EPR in-core neutron measuring system

AN/GV: normal shutdown using steam generators for reactor cooling (French acronym) (*arrêt normal utilisant les générateurs de vapeur*)

AN/RRA: normal shutdown using the residual heat removal system (RHRS) for reactor cooling (French acronym) (*arrêt normal utilisant le circuit RRA*)

AO: Axial Offset; axial distortion of the neutron flux in a reactor core

AP1000: pressurized water reactor of approximately 1150 MWe developed by Westinghouse Electric Corporation

AP-913: Advanced Project 913; method used by EDF to optimize maintenance through reliability in the French nuclear power plant fleet

APOLLO: name of 2D neutron simulation software used for establishing multi-parameter libraries of effective neutron cross-sections

ASAMPSA: Advanced Safety Assessment Methodologies for Probabilistic Safety Assessments; projects concerning probabilistic safety assessments carried out in the European Framework Programme for Research and Technological Development

ASP: Accident Sequence Precursor analysis programme, USA

ASTEC: Accident Source Term Evaluation Code; system of simulation codes for evaluating the physical phenomena occurring during a core-melt accident in a pressurized water reactor

ATF: Advanced Technology Fuel

ATHEANA: A Technique for Human Error ANAlysis; a probabilistic human reliability assessment model

ATMEA1: 1100 MWe pressurized water reactor project developed jointly by Mitsubishi Heavy Industries and Areva

ATPu: plutonium technology facility, now closed; its main activity was the production of MOX (mixed depleted uranium and plutonium) fuel for nuclear reactors (*Atelier de technologie du plutonium*)

ATWS: Anticipated Transient Without Scram (without reactor trip); incident during a transient where rod cluster control assemblies fail to drop

AZALEE: name of a shake table at CEA Saclay, France

BDBA: Beyond-Design-Basis Accident

BEST: BElgian Stress Tests

BETHSY: CEA experiment facility (thermal-hydraulic test loop) (*Boucle d'études de thermohydraulique système*)

BL: Electrical Building (in the French nuclear power plant fleet)

BOC: Beginning of Cycle

BORA-BORA: name of a mock-up used by EDF to study the dispersion and erosion of a 'plug' of unborated water transferred to the core of a pressurized water reactor

BSAF: Benchmark Study of the Accident at the Fukushima Daiichi nuclear power station

BWR: Boiling Water Reactor

CAB (CAB letter): ministerial letters (that set nuclear safety guidelines, for example)

CABRI: test reactor operated by CEA in Cadarache, France, made available to IRSN to study accident situations in pressurized water and fast-neutron reactors

Cast3M: name of a simulation software programme using the finite-element method for structural and fluid mechanics

CATHARE: advanced thermal-hydraulic simulation code used for PWR safety analyses (*Code avancé de thermohydraulique pour l'étude des accidents de réacteurs à eau*)

CCI: name given to cartridge-type sump filters built by Areva (French nuclear power plant fleet)

CCWS: Component Cooling Water System (French nuclear power plant fleet)

C3X ('C cube X'): computation platform used to simulate the dispersion of atmospheric release of radioactive substances on a regional scale (several hundred kilometres around a nuclear facility where an accident has occurred)

CEMETE: EDF test laboratory

CEOS.fr: behaviour and assessment of special structures: cracking and shrinkage (*comportement et évaluation des ouvrages spéciaux : fissuration – retrait*)

CEPP: reactor coolant pump standstill seal system (in French nuclear power plants)

CERES: name of a simulation code for calculating the radiological impact of release in an accident situation

CESAR: module in the ASTEC software suite

CEUS: Central and Eastern United States

CFD: Computational Fluid Dynamics

CFR: Code of Federal Regulations, USA

CFT: Cold Functional Test

CFX, NEPTUNE_CFD, STAR-CD, TrioCFD: CFD-type simulation software codes

Chicago Pile-1: reactor at the University of Chicago, the first atomic pile using natural uranium and graphite

CHRS: ultimate Containment Heat Removal System (the French equivalent for the Flamanville 3 EPR is 'EVU')

CILWDS: Conventional Island Liquid Waste Discharge System (in French nuclear power plants)

CIP: Cabri International Programme; an international programme to study the behaviour of nuclear fuel rods and cladding during a reactivity injection accident in pressurized water reactors

CIP: Complementary Investigation Programme for reactors in the French nuclear power plant fleet) (*Programme d'investigations complémentaires*)

COC: 'pseudo' instrumentation and control system (reactors in the French nuclear power plant fleet)

COMAS: full-scale corium cooling tests performed by Areva

COMET: Name of facility in Germany where reflooding tests were conducted

CONTROBLOC: computerized relay cabinets for programmable logic controllers in reactors of the French 1300 MWe P4 and P'4 nuclear power plants (CONTRONIC for the N4 reactors, SPPA-T2000 for the EPR)

ConVex: emergency response exercises organized by the IAEA

COPAT: reactor outage operations centre (*centre opérationnel de pilotage des arrêts de tranche*)

CP: ‘programme contract’; name given to the various ‘work packages’ for reactors in the 900 MWe series of the French nuclear power plant fleet (see below)

CPA: name of a module in the ASTEC simulation software suite

CP0, CPY (CP1 and CP2): three subfamilies or groups of 900 MWe reactors in the French nuclear power plant fleet (the designation ‘CP0’ was adopted after the reactors in this series had been commissioned)

CP1: full-scale control room simulator at the Bugey nuclear power plant

CRDM: Control Rod Drive Mechanism (French nuclear power plant fleet)

CRIHOM: IRSN database containing internal contamination measurements

CRISTAL: name designating a form used in assessment of criticality risk in all nuclear facilities and transport packages involving fissile materials

CRITER: IRSN database assembling the results of radioactivity measurements carried out in the field (for emergency response purposes)

CRONOS: name of 3D simulation software used to determine the neutronics at work in a reactor core

CRPs: Coordinated Research Projects, IAEA

CSAs: Complementary Safety Assessments conducted in France following the Fukushima Daiichi accident (ECS in French for *évaluations complémentaires de sûreté*)

CSC: Corium Spreading and Coolability project

CSM: Continuous State Monitoring

CSS: containment spray system (‘EAS’ for reactors in the French nuclear power plant fleet except for EPR)

CVCS: Chemical and Volume Control System for reactor coolant of pressurized water reactors in the French nuclear power plant fleet

CWS: circulating water system, in which water passes through the condenser to cool and condense the water vapour (‘CRF’ for reactors in the French nuclear power plant fleet)

CYCLADES: a fuel management regime (fuel cycle to increase availability through safety assessment), for reactors in the French nuclear power plant fleet

DAMAC: portable device for taking measurements on fuel assemblies (*dispositif amovible de mesure des assemblages combustibles*)

DAPE: application submitted to request continued operation of an item of equipment for reactors in the French nuclear power plant fleet *(dossier d’aptitude à la poursuite de l’exploitation d’un équipement*)

DBA: Design-Basis Accident

DBC: Design-Basis Conditions, designation given to reference operating conditions in ASN Guide No. 22 (France)

DBE: Design-Basis Earthquake

DDF: Operating Lifetime Project, name of EDF's plan to extend the operating lifetime of reactors in the French nuclear power plant fleet beyond 40 years (*durée de fonctionnement*)

DEC: Design Extension Conditions ('complementary domain of events', notion similar to 'beyond-design-basis events') (*domaine de conception étendu*)

DEG: nuclear island chilled water system, in particular for the reactor building and fuel building (reactors in the French nuclear power plant fleet, except for EPR)

DENOPI: research programme on fuel assembly uncovery accidents in a spent fuel pool) (*Denoyage piscines*)

DIVA: IRSN experiment facility dedicated to conducting fire tests (*Dispositif incendie, ventilation et aérocontamination*)

DIVA: name of a module in the ASTEC simulation software suite

DN: nominal diameter

DNA: DeoxyriboNucleic Acid

DNBR: Departure from Nucleate Boiling Ratio

DOR: periodic review strategic plan established in preparation for ten-yearly inspections of the French nuclear power plant fleet (*Dossier d'orientation du réexamen*)

D/P AG: method used for diagnostics and prognostics of serious accident situations and their progression (emergency response)

DRACCAR: software used to simulate deformation and reflooding of a fuel assembly during a loss-of-coolant accident (*Déformation et renoyage d'un assemblage de crayons combustibles pendant un accident de refroidissement*)

DRS: Design Response Spectra

DSHA: Deterministic Seismic Hazard Analysis

DVN, DVQ: ventilation systems for the nuclear auxiliaries building and the effluent treatment building (reactors in the French nuclear power plant fleet except for EPR)

EASu: ultimate containment spray system (reactors in the French nuclear power plant fleet except for EPR)

EATF: Enhanced Accident Tolerant Fuel, developed by Areva (which has since become Framatome)

ECCS: Emergency Core Cooling System (Chernobyl)

ECHO 330, single-probe ECHO: ultrasound tools developed by Areva to locate leaking rods in a fuel assembly

ECOSTAR: Ex-vessel COre-melt STAbilization Research

ECP: in the state-oriented approach, set of operating strategies that may be applied to the reactor coolant system in PWR states where the residual heat removal system is not connected (French nuclear power plant fleet) (*état conduite primaire*)

ECPR: in the state-oriented approach, set of operating strategies that may be applied to the reactor coolant system in PWR states where the residual heat removal system is connected and the reactor coolant system is closed (French nuclear power plant fleet) (*état conduite primaire RRA connecté*)

ECPRO: in the state-oriented approach, set of operating strategies that may be applied to the reactor coolant system in PWR states where the residual heat removal system is connected and the reactor coolant system is open (French nuclear power plant fleet) (*état conduite primaire RRA connecté primaire ouvert*)

ECR: Equivalent Cladding Reacted; oxidation rate of cladding during an operating transient such as a loss-of-coolant accident, expressed as a percentage of the cladding thickness

ECRIN: IRSN database providing validated and referenced dose coefficients used to calculate doses received by humans

ECS: in the state-oriented approach, a set of operating strategies that may be applied to the secondary side of a pressurized water reactor (French nuclear power plant fleet) (*état conduite secondaire*)

ECURIE: European Community Urgent Radiological Information Exchange

EDGAR: facility at CEA's Saclay site in France used to study fuel rod behaviour in pressurized water reactors

EDGE: French research project on the interface between experts and decision-makers in emergency response situations in high-risk industries

EFWS: steam generator emergency feedwater system for steam generators (equivalent acronym is ASG in the French nuclear power plant fleet)

EIP: Equipment Important to Protection of 'protected interests' (public security, health and hygiene, protection of nature and the environment, as defined in the French Environment Code) (*élément important pour la protection*)

EIS: Equipment Important to Safety, a concept in French regulations replaced by the notion of 'Equipment Important to Protection' (see above) (*élément important pour la sûreté*)

ELSA: name of a module in the ASTEC simulation software suite

EPIC: French industrial and commercial public undertaking

EPR: European Pressurized water Reactor

EPR 2: upgrade of the NM EPR

EPRESSI: A method for substantiating fire compartmentation based on the performance assessment of actual compartmentation elements used in fire compartmentation

ESCADRE: software suite, now replaced by ASTEC, for studying core-melt accidents

ESWS: Essential Service Water System (used to cool the CCWS for reactors in the French nuclear power plant fleet)

ETB: Effluent Treatment Building (French nuclear power plant fleet)

ETC-C: EPR Technical Code for Civil Works

ETY: containment atmosphere monitoring system that checks hydrogen content and air circulation in the pressurized water reactor building (French nuclear power plant fleet)

EUR: European Utility Requirements

EUROPLEXUS: finite-element software for simulating fast transient dynamics

FARN: Nuclear Rapid Response Force for the French nuclear power plant fleet, planned and implemented by EDF following the accident at the Fukushima Daiichi nuclear power plant) (*force d'action rapide nucléaire*)

FB: Fuel Building (French nuclear power plant fleet)

FG: in an FMEA, a group or Functional Group of equipment (i.e. performing the same function)

FINAS: Fuel Incident Notification and Analysis System, IAEA

FIPLOC: software program for containment thermal hydraulics in the ESCADRE system, now replaced by ASTEC

FLEX: strategy and ultimate emergency measures for nuclear power plants set up in the USA following the Fukushima Daiichi nuclear power plant accident

FLICA: software for simulating the thermal hydraulics of a nuclear reactor core during transients

FMEA: Failure Mode and Effects Analysis

FMECA: Failure Modes, Effects and Criticality Analysis

FP: Fission Product

FPCPS: Fuel Pool Cooling and Purification System in the French nuclear power plant fleet

FPCS: Fuel Pool Cooling System (in French nuclear power plants)

FUCHIA: test programme on the efficiency of sand filters (installed in the French nuclear power plant fleet, except for EPR)

GALICE: fuel management system with limited increase in irradiation for reactors (*Gestion avec augmentation limitée de l'irradiation pour le combustible en exploitation*) in the French nuclear power plant fleet

GARANCE: advanced fuel management system adapted for planned new reactor cores (*Gestion avancée des REP avec adaptation aux nouveaux cœurs envisagés*) in the French nuclear power plant fleet

GCR: gas-cooled (graphite-moderated) reactor, a type of nuclear power reactor in France

GEMMES: system for safe fuel management according to developments and changes in the reactor operating mode (*Gestion des évolutions et des modifications des modes d'exploitation en sûreté*) in the French nuclear power plant fleet

GMPE: Ground Motion Prediction Equations

GPEC: Strategic workforce planning (*gestion prévisionnelle des emplois et des compétences*)

GSG: General Safety Guides (IAEA publications)

GSR: General Safety Requirements (IAEA publications)

GWd: gigawatt-day

GWTS: Gaseous Waste Treatment System (French nuclear power plant fleet)

HELB: High-Energy Line Break

HEMERA: Highly Evolutionary Methods for Extensive Reactor Analyses; computer code used to simulate thermal-hydraulic and neutronic phenomena occurring during nuclear reactor transients

HEPA: High-Efficiency Particulate Arresting filter

HFT: Hot Functional Test

H*n*: accident operating procedures covering beyond-design-basis conditions for reactors in the French nuclear power plant fleet (*hors dimensionnement*)

HOF: Human and Organizational Factors

HORAAM: Human and Organizational Reliability Analysis in Accident Management

HPCI: High-Pressure Coolant Injection System; emergency core cooling system for a boiling water reactor with a higher flow rate than the RCIC (Fukushima Daiichi Nuclear Power Plant)

HRO: High-Reliability Organization

HRP: Halden Reactor Project, Norway

HSO: the name of an EDF initiative to take into account human, social and organizational aspects when modifying facilities and their operating procedures

I&C: Instrumentation and Control

IB: Intermediate Break

IB LOCA: intermediate break loss-of-coolant accident

IC: Isolation Condenser; emergency core cooling system of a boiling water reactor (Fukushima Daiichi Nuclear Power Plant Unit 1, which includes neither RCIC nor HPCI)

ICARE: name of a module in the ASTEC simulation software suite

ICD: International Classification of Diseases

ICPE: facility classified for protection of the environment; concept defined in French regulations (*installation classée pour la protection de l'environnement*)

ICS: In-Core instrumentation System

ICSPs: International Collaborative Standard Problems, IAEA

IDiPS-RPS: Integrated Digital Protection System – Reactor Protection System

I4D: 'Total loss of train A due to fire' (EDF operating procedure)

IGC: InterGranular Corrosion

INB: basic nuclear installation, i.e. a regulated nuclear facility (concept specific to French regulations) (*installation nucléaire de base*)

INBS: basic nuclear installation for defence, i.e. a regulated nuclear facility used for defence purposes (concept specific to French regulations) (*installation nucléaire de base classée secrète*)

INES: International Nuclear Event Scale (developed by the IAEA)

INEX: International Nuclear Emergency Exercise, organized by the OECD

INSC: Instrument for Nuclear Safety Cooperation (European technical assistance programme)

IODE: name of a module in the ASTEC simulation software suite

IPE: Individual Plant Examination, USA

IPEEE: Individual Plant Examination for External Events, USA

IPS: important to safety, replaced by EIPS (concepts defined in French regulations) (*Important pour la sûreté*)

IPS-NC: important to safety, non-safety-grade, i.e. equipment not classified as 'safety-grade' at the initial design stage of existing reactors, although it is important to safety (*important pour la sûreté, non classé*)

IRD: Intermediate Range Detector

IRHR: Independent Residual Heat Removal System

IRS: International Reporting System for Operating Experience; an international system for collecting and publishing information on incidents at nuclear power reactors

IRSRR: Incident Reporting System for Research Reactors; an international system for collecting and publishing information on incidents at nuclear research reactors

IRWST: In-containment Refuelling Water Storage Tank (located inside EPR containment)

ISCA: Independent Safety Culture Assessment, IAEA

ISIS: name of a fire simulation software package

ISODOP: name of a module in the ASTEC simulation software suite

ISTP: International Source Term Program

IT: Information Technology

ITER: International Thermonuclear Experimental Reactor; a Tokamak-type nuclear fusion reactor under construction at CEA Cadarache, France

IVMR: In-Vessel Melt Retention

IVR: In-Vessel Retention

JDT: fire detection system (reactors in the French nuclear power plant fleet)

K1, K2, K3: qualification levels or profiles of equipment for accident conditions (K3AD, K3 conditions in a degraded atmosphere)

KANT: software for development and quantification of event trees

KIC: computerized control system featured on N4 series reactors

KIR: vibration and acoustic monitoring system for detecting loose parts in the nuclear steam supply system (on reactors in the French nuclear power plant fleet)

KIT/KPS: computer equipment featured on the control room safety panel on reactors in the French nuclear power plant fleet

KONVOI: a type of pressurized water reactor of German design (KWU)

KTA: German Nuclear Safety Standards Commission, and the rules established by this committee (*Kerntechnische Ausschuss*)

LB: Large Break

LBB: Leak Before Break

LB LOCA: large break loss-of-coolant accident

LCP: Lower Core Plate in a pressurized water reactor of the French nuclear power plant fleet) (*Plaque inférieure de cœur, PIC*)

Learjet 23: small twin-engine business jet taken into account in the safety analysis of reactors in the French nuclear power plant fleet

LET: Linear Energy Transfer

LGA, LGB, LGC, LGD: electrical switchboards (reactors in the French nuclear power plant fleet)

LHA, LHB: emergency-supplied electrical switchboards (reactors in the French nuclear power plant fleet)

LHP, LHQ, LHT: emergency diesel generators (reactors in the French nuclear power plant fleet)

LHSI: Low-Head Safety Injection of water into the reactor coolant system of a pressurized water reactor

LLS: emergency turbine generator (reactors in the French nuclear power plant fleet)

LNG: Liquified Natural Gas

LNG and LNH: Controbloc system 220 V power supply panels (reactors in the French nuclear power plant fleet)

LNT: Linear No-Threshold model

LOCA: Loss-of-Coolant Accident

LOOP: Loss Of Off-site Power

Low Tin Zirlo™: alloy used for fuel assembly rod cladding produced by Westinghouse

LPD: Linear Power Density released by fuel rods in a reactor

LS: safety-related

LS-DYNA: fast dynamics simulation software for the study of structures

LSS: Life Span Study; study on the consequences of the atomic bombings of Hiroshima and Nagasaki

MAAP: Modular Accident Analysis Program; comprehensive software (or software suite) for simulating physical phenomena during a pressurized water reactor core melt accident

MCCI: Molten Corium-Concrete Interaction

MCE: Maximum Credible Earthquake

MCNP: Monte Carlo N-Particle transport code; 3D simulation code for particle transport based on the Monte Carlo method

MC3D: name of a 3D multi-phase thermal-hydraulic code used to simulate the interaction between molten materials and coolant

MELCOR: integrated software (or software suite) for simulating physical phenomena occurring during a core-melt accident in a pressurized water reactor

MEPEM: model for probabilistic assessment of human failures (*Méthode d'évaluation probabiliste de l'échec des missions*)

MERMOS: model for probabilistic study of human reliability (*Méthode d'évaluation de la réalisation des missions opérateur pour la sûreté*)

MeV: megaelectronvolt

M5®: zirconium alloy developed by Areva

MFWS: steam generator main feedwater system (equivalent acronym is ARE in the French nuclear power plant fleet)

MHPE: Maximum Historically Probable Earthquake

MHSI: Medium-Head Safety Injection of water into the reactor coolant system of a pressurized water reactor

MORET: simulation software that solves the neutron transport equation using Monte Carlo methods, mainly used for criticality studies

MOX: Mixed Oxide Fuel: fuel consisting of a mixture of uranium and plutonium oxides (UO_2 + PuO_2)

MOX Parity: type of fuel management used in reactors in the French nuclear power plant fleet

MPL: maximum permitted levels of radioactivity for the sale of food products

MPS: main primary system (of a pressurized water reactor) (CPP in French)

Ms: surface wave magnitude of an earthquake

MSBa: Main Steam Bypass from the turbine generator to the atmosphere (French nuclear power reactors)

MSBc: Main Steam Bypass from the turbine generator to the condenser (French nuclear power reactors)

MSK: Medvedev-Sponheuer-Karnik scale for measuring earthquake intensity

MSS: main secondary system (of a pressurized water reactor) (CSP in French)

MT: main transformer, supplies power to reactors in the French nuclear power plant fleet (*transformateur principal*)

Mw: moment magnitude of an earthquake

MWd: megawatt-day

N4: 1450 MWe plant series in the French nuclear power plant fleet

NAB: Nuclear Auxiliary Building (French nuclear power plant fleet)

NDT: Non-Destructive Testing

NDTT: Nil Ductility Transition Temperature

NFEP: New Fuel Elevator Platform; Westinghouse equipment for extracting a rod or rods from a robust fuel assembly

NGF, NGFN: official network of altitude markers in mainland France level (*nivellement général de la France*)

Ni (N1, N2, N3): classification level of an item of equipment according to the French pressure equipment decree

NM EPR: New-Model EPR (EPR upgrade)

NP: Nominal Power

NPP: Nuclear Power Plant

NQM: Non-Quality Maintenance

NSE: Nuclear Safety Engineer

NSS: Nuclear Sampling System (French nuclear power plant fleet)

NSSS: Nuclear Steam Supply System

NUREG: Nuclear Regulatory Report (report published by the U.S. NRC)

NVDS: Nuclear Vent and Drain System (French nuclear power plant fleet)

OBE: Operating Basis Earthquake

ODOBA: Observatory of Durability in Reinforced Concrete Structures; research project to study the ageing of structures and pathologies affecting them (*Observatoire de la durabilité des ouvrages en béton armé*)

OLC: Operational Limits and Conditions

OPEX: OPerating EXperience feedback

Optimized Zirlo™: name of a zirconium alloy developed by Westinghouse

ORM: Operating Reactivity Margin; concept used in the operation of RBMK reactors

ORSEC: emergency response organization; since 2006, this has come to represent emergency response provided by the civil defence organization at the *département* level. Comprehensive French emergency response management system (*organisation de secours*)

PANAME: new action plan for improving the Probabilistic Human Reliability Assessment model with transition to the state-oriented approach (*plan d'actions nouvelles pour l'amélioration du modèle EPFH avec passage à l'APE*)

PASSAM: Passive and Active Systems on Severe Accident source term Mitigation; European Commission research project for limiting releases in the event of a nuclear reactor core melt

PBF: Power Burst Facility (US test facility)

PBMP: basic preventive maintenance programme for reactors in the French nuclear power plant fleet (*programme de base de maintenance préventive*)

PCC: Plant Condition Category (1 to 4 for the EPR)

PCI: Pellet-Cladding Interaction

PCI-SCC: Pellet-Cladding Interaction assisted by Stress Corrosion Cracking

pcm: per cent mille

PCMI: Pellet Cladding Mechanical Interaction

PDS: Plant Damage State; concept used in EPR Level 2 probabilistic safety assessments

PEPSSI: Method used to assess the adequacy of fire compartmentation (*Principe d'évaluation pour la suffisance des éléments de sectorisation incendie)*

PERFROI: Research programme on the risk of fuel ejection from a fuel rod (IRSN, EDF, CNRS) (*Étude de la perte de refroidissement*)

P4: 1300 MWe reactor plant series in the French nuclear power plant fleet

P'4: 1300 MWe reactor plant series in the French nuclear power plant fleet

PGA: Peak Ground Acceleration

PHARE: Poland and Hungary Assistance for Restructuring their Economies (European technical assistance programme)

PHEBUS: CEA experimental reactor used by IRSN for safety tests at the Cadarache site in France

Phébus-CSD: international research programme for the study of significant fuel degradation, based on tests carried out in the PHEBUS reactor

Phébus-FP: international research programme on the behaviour of fission products during pressurized water reactor core melt

PHENIX: decommissioned fast neutron reactor at the Marcoule site in southern France

PHRA: Probabilistic Human Reliability Assessment

PIS: Process Instrumentation System in reactors in the French nuclear power plant fleet

PKL: *Primärkreislauf* (primary system); large-scale German test facility and research projects for the study of the thermal-hydraulic behaviour of a nuclear reactor in an accident situation

PLC: Programmable Logic Controller

PLEXUS, PLEXUS-3C: finite-element software for simulating fast dynamics phenomena

PNGMDR: French national radioactive materials and waste management programme (*plan national de gestion des matières et des déchets radioactifs*)

PPI: off-site emergency plan, France (*plan particulier d'intervention*)

P^{2}REMICS: software for simulating explosions

PRD: Power Range Detector

PRI: Potential Risk Index

PRMS: Plant Radiation Monitoring System in reactors in the French nuclear power plant fleet

PRT: Pressurizer Relief Tank on a pressurized water reactor (French nuclear power plant fleet)

PSA: Probabilistic Safety Assessment

PSA 1: Level 1 PSA

PSA 2: Level 2 PSA

PSHA: Probabilistic Seismic Hazard Analysis

PSR: Periodic Safety Review

PUI: on-site emergency plan for basic nuclear installations in France (*plan d'urgence interne*)

PWR: Pressurized Water Reactor

PWR-Na: tests on PWR fuel rods in the sodium loop of the CABRI reactor

RALOC: one of the software programs for containment thermal hydraulics in the ESCADRE system (now replaced by ASTEC)

RAPSODIE: decommissioned fast-neutron reactor located at the Cadarache site in southern France

RB: Reactor Building (French nuclear power plant fleet)

RBMK: *Reaktor Bolshoy Moshchnosti Kanalnyi* (type of reactor of Soviet design)

RCC: design and construction rules applicable to the French nuclear power plant fleet

RCCA: Rod Cluster Control Assembly

RCC-C: design and construction rules relating to fuel applicable to the French nuclear power plant fleet

RCC-CW: rules for design and construction of civil works on PWR nuclear islands in the French nuclear power plant fleet (including the EPR and earlier reactors during periodic reviews)

RCC-E: design and construction rules for electrical components and instrumentation & control systems in PWR nuclear islands in the French nuclear power plant fleet

RCC-G: design and construction rules for civil works applicable to the French nuclear power plant fleet

RCC-I: design and construction rules for fire protection

RCC-M: design and construction rules for mechanical equipment applicable to the French nuclear power plant fleet

RCCM-MRx: design and construction rules for fast neutron reactors, research reactors and nuclear fission installations

RCC-P: design and construction rules for 'process' design applicable to the French nuclear power plant fleet

RCIC: Reactor Core Isolation Cooling system; emergency core cooling system of a boiling water reactor (Fukushima Daiichi Nuclear Power Plant)

RCLS: EPR Reactor Core Limitation System

RCM: Reliability-Centred Maintenance, EDF

RCP: Reactor Coolant Pump (reactors in the French nuclear power plant fleet)

RCRS: Periodic review final report (French nuclear power plant fleet) (*rapport de conclusions d'un réexamen de sûreté*)

RCS: Reactor Coolant System

REA: water and boron makeup system (in French nuclear power plants)

Recuperare: name of an approach used by IRSN to analyse how operators ‘recover’ event situations

RFA: Robust Fuel Assembly, produced by Westinghouse and loaded in French nuclear power reactors

RFS: fundamental safety rules, France (*règles fondamentales de sûreté*)

RG: Regulatory Guide, USA

RGE: General Operating Rules (*règles générales d’exploitation*)

RHRS: Residual Heat Removal System (French nuclear power plant fleet)

RIC: reactor in-core measurement instrumentation system (French nuclear power plant fleet)

RJH: Jules Horowitz Reactor

RPR: French three-letter code for the Reactor Protection System (French nuclear power plant fleet)

RPV: Reactor Pressure Vessel

RRC-A: Risk Reduction Category A; includes multiple failure situations (EPR)

RRC-B: Risk Reduction Category B; includes situations with core melt (EPR)

RSE-M: mechanical equipment in-service monitoring rules for reactors in the French nuclear power plant fleet (*règles de surveillance en exploitation des matériels mécaniques*)

RSNR: research on nuclear safety and radiation protection (French National Research Agency)

RT: Reactor Trip (French nuclear power plant fleet)

R3F: low-leakage operating rule for steam generators in reactors in the French nuclear power plant fleet (*règle de fonctionnement dit à faible fuite*)

RUPUICUV: name of a module in the ASTEC simulation software suite

S1, S2 and S3: names given, in the 1970s, to three types of radioactive release to the environment in core-melt situations

SAB: Safeguard Auxiliary Building (certain reactors in the French nuclear power plant fleet)

SAG: Safety Assessment Guide

SALP: Systematic Assessment of Licensee Performance, USA

SALTO: Safety Aspects of Long Term Operation (service offered by the IAEA)

SAPHIR: event file managed by EDF

SAR: instrument compressed air system (reactors in the French nuclear power plant fleet)

SAR: Safety Analysis Report (also Final Safety Analysis Report)

SARNET: Severe Accident Research NETwork of excellence

SB LOCA: Small-Break Loss-of-Coolant Accident

SBO: Station Blackout

SBO DG: Station Black-Out Diesel Generator

SCANAIR: software for simulating the thermal-mechanical behaviour of fuel rods in pressurized water reactors during power transients

SCC: Stress Corrosion Cracking

SEP: Systematic Evaluation Process, USA

SESAME: software suite for computing accident situation progression and assessment methods (*Schéma d'évolution des situations accidentelles et moyens d'évaluation)*

SEXTEN: containment integrity monitoring system (reactors in the French nuclear power plant fleet)

SF: Safety Fundamentals (IAEA publications)

SFu: ultimate heat sink (*source froide ultime*)

SG: Steam Generator

SGBS: steam generator blowdown system (French nuclear power plant fleet)

SGTR: Steam Generator Tube Rupture

SI: Safety Injection of water into the reactor coolant system of a pressurized water reactor

SIGMA: Seismic Ground Motion Assessment; research and development programme for the assessment of seismic ground motion

SINAPS@: seismic events and nuclear facilities: improving and sustaining safety, a French research project (*Séisme et installation nucléaire: améliorer et pérenniser la sûreté*)

SIP: Shelter Implementation Plan; plan launched in 1997 for the containment of the damaged reactor at the Chernobyl nuclear power plant

SIS: Safety Injection System (French nuclear power plant fleet)

SLB: Steam-Line Break

SM: Shift Manager

SME: Seismic Margin Earthquake

SMR: Small Modular Reactor

SNETP: Sustainable Nuclear Energy Technology Platform

SOA: state-oriented approach

SOFIA: simulator for observation of PWR incident and accident operation used by IRSN (*Simulateur d'observation du fonctionnement incidentel et accidentel)*

SOPHAEROS: name of a module in the ASTEC simulation software suite

SPERT: Special Power Excursion Reactor Test (US test reactor)

SPI: Continuous post-incident monitoring, a procedure used for reactors in the French nuclear power plant fleet, replaced by continuous state monitoring in the State-Oriented Approach (*surveillance permanente après incident*)

SPND: Self-Powered Neutron Detectors; EPR in-core neutron detector measuring system

SPOT: VVER-1200 system for passive cooling of steam generators in the event of total loss of power supply

SPU: emergency procedure for continuous monitoring of the reactor state in a declared emergency situation (French nuclear power plant fleet) (*surveillance permanente ultime*)

SRC: source range (neutron measurement) channel (reactors in the French nuclear power plant fleet)

SRD: Source Range Detector

SSC: Structures, Systems and Components

SSFI: Safety System Functional Inspection, USA

SSG: Specific Safety Guide, IAEA

SSR: Specific Safety Requirements (IAEA publications)

SSSS: StandStill Seal System on reactor coolant pumps (French nuclear power plant fleet)

ST: step-down transformer for reactors in the French nuclear power plant fleet (*transformateur de soutirage*)

STAR: EDF tool for a fuel assembly skeleton replacement

S3C: reactor control room simulator developed by EDF for the N4 series of nuclear power plants, used for ergonomic assessments

SUNSET: Sensitivity and UNcertainty Statistical Evaluation Tool (name of an IRSN statistics tool)

SUPERPHENIX: decommissioned sodium-cooled fast neutron reactor at the Creys-Malville nuclear power plant, France

SYLVIA: software suite for studying ventilation, fire and airborne contamination

SYSINT: name of a module in the ASTEC simulation software suite

TACIS: Technical Assistance to the Commonwealth of Independent States and Georgia (European Technical Assistance Programme)

TAM: equipment hatch providing access to reactor containment in the French nuclear power plant fleet (*tampon d'accès des matériels*)

TECDOC: TEChnical DOCument published by the IAEA

TECV: French Act No 2015-992 on energy transition for green growth, adopted on 17 August 2015

THERP: Technique for Human Error-Rate Prediction (US model for probabilistic human reliability assessments)

THNGV: very high level of water in a steam generator (*très haut niveau dans un générateur de vapeur*) (steam generator EFWS isolation threshold) (French nuclear power plant fleet)

3D/3P: French approach to diagnostics and prognostics applied to the progression of an accident situation in emergency response management

TMI: Three Mile Island, a nuclear power plant located in the USA

TMI-2: Three Mile Island Nuclear Power Plant Unit 2

TOPFLOW-PTS: Experiment facility located in Germany (Helmholtz-Zentrum Dresden-Rossendorf)

TrioCFD: computational fluid dynamics simulation software

TRIPOLI: three-dimensional polykinetic simulation software that uses the Monte Carlo method to solve the coupled neutron-photon transport equation (*Tridimensionnel polycinétique*)

TSAG: Technical Safety Assessment Guide (ETSON)

TSN Act: Nuclear Transparency and Security Act No. 2006-686 of 13 June 2006, France

TUY: commissioning test programme for piping in the reactor coolant, secondary and auxiliary systems on reactors in the French nuclear power plant fleet

UCP: Upper Core Plate of a pressurized water reactor in the French nuclear power plant fleet) (*plaque supérieure de cœur*)

UDG: Ultimate Diesel Generator

U5: emergency operating procedure for reactors in the French nuclear power plant fleet (except for EPR)

U*n*: 'ultimate' emergency operating procedures for reactors in the French nuclear power plant fleet

UNGG: natural uranium, graphite and gas (*uranium naturel, graphite et gaz)*

USA: United States of America

UTO: EDF Corporate Technical Support Department (*unité technique opérationnelle*)

UVCEs: Unconfined Vapour Cloud Explosions

VCT: Volume Control Tank (in French nuclear power plants)

VD: ten-yearly inspection programme. By extension, 'ten-yearly outage' refers to the outage during which this inspection programme takes place (*visite décennale*)

VERCORS: CEA facility in Grenoble, France that performs tests to study the release of fission products from irradiated fuel subjected to a temperature rise

VERCORS: Realistic Verification of Reactor Containment; EDF mock-up and tests for assessing leaks through the reactor containment in accident situations (*Vérification réaliste du confinement des réacteurs*)

VERDON: CEA experiment facility that replaced the VERCORS facility in Grenoble

VIKTORIA: an experimental loop in Levice, Slovakia to research water recirculation in a pressurized water reactor in an accident situation

V-LOCA: loss-of-coolant accident outside the containment that may lead to direct release into the environment

VULCANO: Versatile UO_2 Laboratory for Corium ANalysis and Observation, CEA facility for researching vessel failure and erosion of the basemat by molten corium in a reactor core-melt accident

VVER: Russian power reactor using water as coolant and moderator (*Vodo-Vodianoï Energuetitcheski Reaktor*)

WASH: abbreviation for Washington, used as prefix in publications issued by the US Atomic Energy Commission, dissolved in 1974

Zircaloy-4: a zirconium alloy

Zirlo™: name of a zirconium alloy developed by Westinghouse

ZOÉ: first atomic pile in France

*
*   *

Technical glossary

Some of the technical acronyms listed above, which largely relate to reactor physics and reactor protection systems, are clarified below.

βeff: proportion of delayed neutrons in a nuclear reactor core (reactor physics concept).

CCWS: the Component Cooling Water System of reactors in the French nuclear power plant fleet cools the fluid of most of the auxiliary and emergency systems of the nuclear steam supply system; it is cooled by the Essential Service Water System.

CVCS: the Chemical and Volume Control System for reactor coolant in pressurized water reactors in the French nuclear power plant fleet is an auxiliary system that ensures water makeup (particularly during reactor heating and cooling phases, in order to compensate for the expansion or contraction of water in the reactor coolant system as the temperature varies), controls the boric acid content of water in the reactor coolant system, purifies and controls water chemistry, activates auxiliary spraying of the pressurizer when the reactor coolant pumps are stopped and supplies water to the reactor coolant pump seal system.

F_Q, $F_{\Delta H}$: 'hot spot' factors for fuel rods in a nuclear reactor core (reactor physics concept).

Fxy(z): radial shape (or distribution) factor of the power in a nuclear reactor core; applies to the power of the rods at elevation *z* (reactor physics concept).

G3: name of a 'calibration curve' used for reactors in the French nuclear power plant fleet. This curve compensates for instantaneous variations in core reactivity resulting from power variations, without distorting power distribution in the core.

keff: effective neutron multiplication factor (reactor physics concept).

KIT/KPS: this computer equipment, mounted in the safety panel of the reactor control room in the French nuclear power plant fleet, provides assistance to the operator in an accident situation by grouping together, in composite or itemized indications, the various items of information available in the control room, including data from the core cooling monitor.

ℓ: mean neutron lifetime (time interval between two generations of neutrons, a reactor physics concept).

LHT: in the event of failure of the turbine-driven pump, the LHT emergency diesel generator for reactors in the French nuclear power plant fleet ensures that water is supplied to the steam generators by means of a motor-driven pump belonging to the emergency feedwater system.

NPSH: Net Pressure Suction Head is the minimum value of the suction pressure of a pump below which there is a risk of cavitation.

NVDS: the Nuclear Vent and Drain System of reactors in the French nuclear power plant fleet collects liquid and gaseous effluents produced by the nuclear systems and facilities in a reactor that may contain radioactive substances.

pH: hydrogen potential of a solution (acid, neutral, basic).

ϕ: flux (neutron or heat flux, number or power per unit of surface area).

PIS: the Process Instrumentation System on reactors in the French nuclear power plant fleet acquires the information delivered by the thermodynamic analogue measurement sensors (pressure, temperature, flow, etc.) and translates them into an electrical signal (through scaling, current-voltage transformation, etc.). In the case of 900 MWe reactors, the PIS also detects when thresholds have been exceeded and sends the corresponding 'binary' information to the Protection System; in other French nuclear power reactors, the PIS sends the 'analogue' measurements to the Protection System, which then determines whether any thresholds have been exceeded. The corresponding system on the EPR is the Process Instrumentation Preprocessing System (PIPS).

PKL: experimental loop (and its associated programmes) at Framatome in Erlangen, Germany, used to study various phenomena of non-homogeneity in the reactor coolant and secondary systems of a pressurized water reactor, for example the transfer of a 'plug' of unborated water or cold water to the core.

Process: in the field of nuclear reactors, 'process' is a term used by designers to refer to the entire heat generation and extraction system, including the electrical power generation system in the case of a nuclear power reactor.

PS: the main functions of the reactor Protection System in the French nuclear power plant fleet are to detect abnormal situations, automatically shut down the reactor and activate the appropriate safety systems in accident situations. It receives neutron and thermal-hydraulic measurements (or information about out-of-limit conditions in the case of 900 MWe reactors – see PIS) and prepares the shutdown and safeguard commands according to the combinations of set points that have been exceeded in redundant measurement channels, any inhibitions and safe settings of certain measurements, and 'permissive signals' characterizing the state of the reactor.

Pth: thermal power (generally expressed in MW) released in a reactor core.

RAM: the power supply system for the control rod drive mechanisms of the reactors in the French nuclear power plant fleet includes motors powered by the external electrical power grid with flywheels, which generate an electrical current.

RCLS: the purpose of the EPR's Reactor Core Limitation System is to avoid triggering the protection functions by initiating actions on the rod cluster control assemblies in order to keep reactor parameters below the activation thresholds of the protection functions.

Rho (ρ): neutron reactivity of a nuclear reactor core (reactor physics concept).

SARNET: the Severe Accident Research Network of Excellence was launched in April 2004 under the European Commission's Research and Development Framework Programmes. Coordinated by IRSN, SARNET brings together some fifty organizations (safety institutes, universities, industry, research centres, etc.) from about twenty European countries as well as the USA, Canada, South Korea, India and Japan.

SIS: the Safety Injection System of reactors in the French nuclear power plant fleet sends water into the core to cool it down in the event of a rupture (or major break) in the reactor coolant system.

T: this symbol designates the neutron period of a nuclear reactor (reactor physics concept).

Tsat: saturation temperature of water in a pressurized water reactor *(ΔTsat*: subcooling margin – a physics concept used to control pressurized water reactors).

U5: procedure for accident operation of reactors in the French nuclear power plant fleet (except for the EPR) which decompresses the containment atmosphere in core-melt situations and filters any release.

Science and Technology Series

ELEMENTS OF NUCLEAR SAFETY PRESSURIZED WATER REACTORS

Jean Couturier, Coordinator

Everything that is important to know about pressurized water reactor safety in nuclear power plants is compiled in this work of reference, from safety fundamentals and reactor design to provisions for managing a radiological or nuclear emergency. The book narrates the determined and continuous quest to enhance nuclear safety. Jean Couturier, coordinator and senior editor, covers the forty-year history of evolution in the safety objectives, approaches, analysis methods and assessment criteria that have defined pressurized water reactor safety, mainly within the French nuclear power plant fleet, from the 1970s up to today's Flamanville 3 EPR. Everyone, including current and future generations of engineers, researchers and, more broadly, any citizen interested in nuclear safety issues will find that the book reinforces their knowledge on this important subject, providing an understanding of the fundamentals, to the benefit of nuclear and radiological risk control.

ISBN : 978-2-7598-2722-0

9 782759 827220

IRSN
INSTITUT DE RADIOPROTECTION
ET DE SÛRETÉ NUCLÉAIRE

31, avenue de la Division Leclerc
92260 Fontenay-aux-Roses
RCS Nanterre B 440 546 018

POSTAL ADDRESS
B.P. 17 - 92262 Fontenay-aux-Roses Cedex

PHONE
+33 (0)1 58 35 88 88
WEBSITE
www.irsn.fr
E-MAIL
contact@irsn.fr
@irsn france