AUTORITÉ DE SÛRETÉ NUCLÉAIRE

ASN GUIDE

BNI

Design of Pressurised Water Reactors

Produced jointly with
the Institut de Radioprotection et de Sûreté Nucléaire

IRSN
INSTITUT DE RADIOPROTECTION ET DE SÛRETÉ NUCLÉAIRE

GUIDE No. 22

Version of 18/07/2017

Preamble

The ASN collection of guides is intended for professionals concerned by the nuclear safety and radiation protection regulations (licensees, users or transporters of ionising radiation sources, general public, etc.). These guides can also be issued to the various stakeholders, such as the local information committees (CLIs).

Each guide sets out recommendations with the aim of:
- explaining the regulations and the rights and obligations of the persons concerned by the regulations;
- explaining the regulatory objectives and, as applicable, describing the practices considered by ASN to be satisfactory.
- giving practical tips and information concerning nuclear safety and radiation protection:

This guide was developed jointly by ASN and the Institut de Radioprotection et de Sûreté Nucléaire (IRSN) and presents recommendations for the design of PWRs.

It takes into account more specifically the safety requirements for reactor design taken from the publications of the International Atomic Energy Agency (IAEA) and the reference levels, safety objectives or recommendations published by the Western European Nuclear Regulators Association (WENRA).

This document is an English translation of the original guide in French which is to be referred to for a guaranteed content.

Contents

I INTRODUCTION

I.1 Context and regulatory references

The following regulatory and guidance texts have been taken into consideration in the preparation of this guide:

- Council Directive 2014/87/Euratom of 8th July 2014 amending Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations.
- the Environment Code and more specifically:
  - chapter III of title IX of book V;
  - articles R. 557-9-1 et seq., R. 557-12-1 et seq. and R. 557-14-1 et seq.;
- the Public Health Code;
- the Labour Code;
- decree 99-1046 of 13th December 1999 relative to nuclear pressure equipment;
- decree 2007-1557 of 2nd November 2007 amended, relative to basic nuclear installations and to regulation of the transport of radioactive substances in terms of nuclear safety;
- the order of 10th November 1999 amended relative to the monitoring of operation of the main primary system and the main secondary systems of nuclear pressurized water reactors;
- the order of 12 December 2005 amended relative to nuclear pressure equipment;
- the order of 7th February 2012 setting out the general rules for basic nuclear installations;
- the order of 30 December 2015 relative to nuclear pressure equipment;
- ASN resolution 2014-DC-0417 of 28th January 2014 concerning the rules applicable to basic nuclear installations (BNI) with regard to the control of fire risks;
- ASN resolution 2014-DC-0462 of 7th October concerning the control of the criticality risk in basic nuclear installations;
- ASN Resolution 2015-DC-0532 of 17th November 2015 relative to the safety analysis report for basic nuclear installations
- the technical guidelines (DT) for the design and construction of the next-generation of nuclear power plants with pressurised water reactors, adopted during the plenary meetings of the French Advisory committee of experts for nuclear reactors and German experts on 19th and 26th October 2000;
- the basic safety rules (RFS) and guides applicable to pressurised water reactors (PWR) published by ASN (see appendix 3).

In addition, the safety objectives for new nuclear power plants[1] and the reference levels[2] published by the Western European Nuclear Regulators Association (WENRA) and the IAEA safety standards (SSR-2/1 in particular[3]) have been taken into account.

[1] "*WENRA statement on safety objectives for new nuclear power plants*", published in November 2010
"*WENRA-RHWG Report - Safety of new NPP designs*", published in August 2013

[2] "*Report - WENRA Safety Reference Levels for Existing Reactors*", published in September 2014

[3] "*Safety of nuclear power plants: design*", Specific Safety Requirements IAEA, No. SSR-2/1, first revision published in February 2016

I.2 Purpose of the guide

This guide addresses aspects relative to the design of the installations, which shall be based on appropriate application of the principle of defence in depth and aspects relative to the demonstration of the nuclear safety of a design, which presupposes that a design has been chosen. In practice, due to the need to produce a design of demonstrable safety, the design analysis and the demonstration of nuclear safety analyses are carried out through an iterative process. In view of the nature of this document, the part concerning the demonstration of nuclear safety is particularly detailed, on the understanding that the appropriateness of a new design shall first be examined from the aspect of applying the principle of defence in depth.

This guide presents the recommendations of ASN and IRSN for the design of pressurised water reactors (PWR[4]). Its primary objective is to address the prevention5 of radiological incidents and accidents and the limitation of their consequences. It also addresses other aspects associated with the management of non-radiological risks or the adverse effects that will result from operation of the facility.

Article L. 593-6 of the Environment Code

The licensee of a basic nuclear installation is responsible for the control of the risks and inconveniences that its installation can present.

It has been drawn up on the basis of knowledge resulting from examinations carried out on the nuclear power reactors in operation, under construction, or at the project stage in France. This guide takes into account the lessons drawn from the reviews of the technical files submitted to ASN by the French applicants which have highlighted the relevance of certain practices. It will be updated regularly to take into account new knowledge, experience feedback (as much from its application to concrete examples as from operation of the facilities), recommendations made by international organisations and new practises. To take such changes into account, ASN may issue additional - or even alternative - recommendations before the next revision of the guide.

It is intended for future PWR licensees in France, responsible for controlling the risks and inconveniences that the installation can present in accordance with article L. 593-6 of the Environment Code, as well as for the authors of specifications and the designers of such installations without prejudice to the responsibilities of the nuclear pressure equipment (NPE) manufacturers provided for by the regulations.

This guide sets out, through inset text boxes, the regulatory requirements to take into account in the design, while the main body of the text presents the recommendations that enable these requirements to be satisfied, as much from the technical aspects as from the relevant organisational and human factors aiming to protect the interests mentioned in the first paragraph of article L. 593-1 of the Environment Code.

[4] See definition in appendix 1.

[5] In the remainder of the guide, "prevent" and "prevention" are to be taken as meaning the search for measures aiming at avoiding an event or a situation, without necessarily succeeding.

These recommendations focus in particular on the objectives, requirements and criteria that the applicants should set for the design of the installation in order to comply with the general objectives set by the regulations.

The recommendations formulated in this guide use the word "shall" in the present tense even though they are not binding.

Article L. 593-1 of the Environment Code

Basics nuclear installations listed in article L. 593-2 are subject to the legal system defined by the provisions of this Chapter and of Chapter VI of this Part due to risks or inconveniences they can represent for public health and safety or protection of nature and the environment.

Article L. 593-42 of the Environment Code

The general rules, prescriptions and measures taken in application of this chapter and of chapters V and VI for the protection of public health, when they concern occupational radiation protection, concern the collective protection measures which are the responsibility of the licensee and designed to ensure compliance with the principles of radiation protection defined in article L. 1333-2 of the Public Health Code.

They apply to the design, operation and decommissioning phases of the installation and are without prejudice to the obligations incumbent on the employer in application of articles L. 4121-1 et seq. of the Labour Code.

I.3 Scope of the guide

This guide applies to PWRs. It essentially addresses the prevention of radiological incidents and accidents and the limitation of their consequences, knowing that other aspects (relating to the management of non-radiological risks or the drawbacks that will result from normal operation of the installation, radiation protection and safety of workers) are to be considered in the design of PWRs.

As this guide applies primarily to the design of new-generation PWRs, its recommendations may also be used, for reference, to seek improvements to be made to reactors in operation, for example during their periodic safety reviews, in accordance with article L. 593-18 of the Environment Code and articles 8a and 8c introduced by the European Directive of 8th July 2014.

Article L. 593-18 of the Environment Code

The licensee of a basic nuclear installation carries out periodic safety review of its installation taking the best international practices into consideration.

This review is designed to allow the situation of the installation to be assessed with respect to the rules applicable to it and must make it possible to update the assessment of the risks or drawbacks the installation presents for the interests mentioned in article L. 593-1, by taking into account in particular of the state of the installation, the experience learned from operation, and the development of knowledge and of the rules applicable to similar installations.

Council Directive 2014/87/EURATOM of 8th July 2014 amending Directive 2009/71/EURATOM establishing a Community framework for the nuclear safety of nuclear installations.

Article 8a

Nuclear safety objective for nuclear installations

1. The member States ensure that national framework for nuclear safety requires that nuclear installations be designed, situated, built, commissioned, operated and delicensed with the objective of preventing accidents and, if an accident should occur, of mitigating its consequences and avoiding:
    a. early radioactive releases that would require off-site emergency measures but with insufficient time to implement them;
    b. large-scale releases that would require protective measures that could not be limited in area or time.
2. Member States shall ensure that the national framework requires that the objective set out in paragraph 1:
    a. applies to nuclear installations for which a construction license is granted for the first time after 14th August 2014;
    b. is used as a reference for the timely implementation of reasonably practicable safety improvements to existing nuclear installation, including in the framework of the periodic safety reviews as defined in article 8c(b).

Article 8c

Initial assessment and periodic safety reviews

The member States shall ensure that the national framework requires that:

a. …

b. the license holder under the regulatory control of the competent regulatory authority, re-assesses systematically and regularly, at least every 10 years, the safety of the nuclear installation as laid down in Article 6(c). That safety reassessment … identifies further safety improvements by taking into account … the most recent research results and developments in international standards, using as a reference the objective set in article 8a.

I.4 Status of the guide

At the date of its publication, this guide shall be considered in priority for the PWRs whose creation authorisation decree has not yet been issued.

Compliance with the recommendations of this guide is considered to be a satisfactory way of meeting the regulatory requirements concerning nuclear safety. It is nevertheless possible to depart from the recommendation if it is proved that the regulatory requirements are satisfied by other means. If there are no recommendations on a specific subject, the acceptability of the licensee's proposal for a given project will be assessed in the examination of the file concerning that project.

This guide underwent a consultation by the stakeholders, including the basic nuclear installation licensees, in September 2016, followed by an examination by the French Advisory committee of experts for nuclear

reactors (GPR) with the participation of members of the French Advisory committee of experts for nuclear pressure equipment (GPESPN).

I.5 Structure of the guide

The guide is structured in 8 parts:

1) this part (part I) is the introduction to the guide; it also contains the definitions specific to the guide;
2) part II presents the design objectives and general principles;
3) part III concerns the demonstration of nuclear safety;
4) part IV addresses general recommendations for the design;
5) part V addresses specific recommendations for the design of barriers;
6) part VI addresses recommendations specific to certain safety functions;
7) part VII sets out other specific recommendations for the design;
8) part VIII concerns the design documents.

It also features four appendices:

- Appendix 1: Definitions
- Appendix 2: Correspondence with the terminology used in the international texts (IAEA, WENRA)
- Appendix 3: RFS and ASN guides applicable on the date of publishing of this document
- Appendix 4: List of acronyms

I.6 Definitions

1.6.1 The terms "*nuclear safety*" and "*radiation protection*" have the meaning set in article L. 591-1 of the Environment Code. The corresponding definitions are reproduced in appendix 1 of this guide; nuclear safety thus covers the prevention and mitigation of the consequences of accidents, whether radiological or not. As indicated in chapter I.3, the majority of the recommendations in this guide address the prevention and mitigation of the consequences of radiological accidents.

Article L. 591-1 of the Environment Code

Nuclear safety comprises all the technical provisions and organisational measures relating to the design, construction, operation, shutdown and decommissioning of basic nuclear installations, as well as the transport of radioactive substances which are adopted with a view to preventing accidents or mitigating their consequences.

Radiation protection is protection against ionising radiation, in other words all the rules, procedures and prevention and surveillance means aimed at preventing or reducing the harmful effects of ionising radiation caused to people, directly or indirectly, including by their adverse environmental impact.

In the remainder of the guide, unless otherwise specified, the term "safety function" refers to a nuclear safety function with respect to the radiological risk.

The terms "*PWR*" and "*cliff-edge effect*" have the meaning set by the *journal officiel de la République Française* in the issues dated 22nd September 2000 and 31st May 2012 respectively. The corresponding definitions are reproduced in appendix 1 of this guide.

The terms *"activity important for protection", "internal hazard", external hazard", internal failure", demonstration of nuclear safety", "effluent", radioactive effluent", "element important for protection", "initiating event", "specified requirement", "licensee", "organisational and human factors", "normal operation", "incident or accident", "emergency situation", "hazardous substance", "area where nuclear waste production is possible"* have the meaning set in article 1.3 of the order of 7th February 2012. The corresponding definitions are reproduced in appendix 1 of this guide.

The terms *"core", "conservative", "criticality", "reactivity,* and *"sub-critical"* are those of the nuclear engineering vocabulary published in the *journal officiel de la République Française* as at the date of publication of this guide. The corresponding definitions are reproduced in appendix 1 of this guide.

In the remainder of this guide, unless otherwise specified, the term EIP (element important for protection) is to be understood as an EIP that is necessary for the demonstration of nuclear safety for radiological risks. To facilitate reading:

- if the text concerns an EIP that is a structure or a component considered individually, the term "structure IP" (i.e. structure Important for Protection) or "component IP" may be used;
- if the text concerns all the EIPs in a system, the term "system IP" may be used.

1.6.2 The expressions *"aggravating failure", "design-basis hazard", "design-basis condition", "single failure criterion", "single failure", "single active failure", "single passive failure", controlled state", "safe state", "single initiating event (SIE)", "safety function", "support function", "integrity of a barrier", "analysis method", "reasonably practicable", "plausible situation"* are defined in appendix 1.

1.6.3 A correspondence between the terms used in this guide and the terminology used in the other international publications is provided in appendix 2 of the guide.

II DESIGN OBJECTIVES AND GENERAL SAFETY PRINCIPLES

II.1 General objectives

II.1.1 Normal operation of the installation

2.1.1.1 In application of article L. 1333-2 of the Public Health Code, one of the design objectives is for the radiological exposure of persons, including through adverse environmental impacts, to be as low as practicable under economically acceptable conditions, both inside and outside the installation.

Article L. 1333-2 of the Public Health Code

Nuclear activities satisfy the following principles: […] 2° The principle of optimisation, whereby the level of exposure of individuals to ionising radiation resulting from one of these activities, the probability of such exposure occurring and the number of persons exposed must be maintained at a level that is as low as reasonably achievable, in view of the state of technical knowledge, economic and societal factors, etc.

2.1.1.2 In application of I of article 4.1.1 and II. of article 6.1 of the order of 7th February 2012, one design objective is to limit:

- the quantities and the chemical and radiological toxicity of liquid and gaseous effluent discharges;
- the quantities and activities of radioactive waste;

associated with normal operation of the installation by using the best available techniques, within the meaning of appendix 1 of the order of 26th April 2011, taking into consideration the characteristics of the installation, its geographical situation and the local environmental conditions. This objective enters into the framework of optimising effluent and waste production which takes into account radiation protection considerations.

Article 4.1 of the order of 7th February 2012

I. - The inconveniences mentioned in article 1.2 include firstly the impacts of the installation on health and the environment due to the water intakes and discharges, and secondly the detrimental effects it can have, such as the dispersion of pathogenic micro-organisms, noise, vibration, odours and dust.

II. - With regard to the abovementioned inconveniencies, the best available techniques mentioned in article 1.2 are those defined by the abovementioned order of 26th April 2011 in the version mentioned in appendix I.

Article 4.1.1 of the order of 7th February 2012

I. - The licensee takes all necessary measures from the design stage to limit effluent discharges from the installation.

Article 6.1 of the order of 7th February 2012

II. - The licensee takes all necessary measures as from the design stage to prevent and reduce, particularly at source, the production and the harmfulness of the waste produced in its installation.

III. - With regard to waste management, the best available techniques mentioned in article 1.2 are those defined by the abovementioned order of 26th April 2011 in the version mentioned in appendix 1.

Appendix 1 of the order of 26th April 2011 relative to the implementation of the best available techniques provided for in article R. 512-8 of the Environment Code

The best available techniques …. are defined as the most effective and advanced stage of development of the activities and their modes of operation, demonstrating the practical ability of particular techniques to constitute, in principle, the basis of maximum emission values aiming at avoiding and, when this proves impossible, generally reducing the emissions and the impact on the environment as a whole.

The term "techniques" covers equally well the techniques used as the manner in which the installation is designed, constructed, maintained, operated and shut down.

The term "available" means the techniques developed on a scale allowing them to be applied in the context of the industrial or agricultural sector concerned, under economically and technical viable conditions, taking into consideration the costs and advantages, whether these techniques are used or produced on the territory of the member State concerned, insofar as the licensee concerned can have access to them under reasonable conditions.

The term "best" means the most effective techniques for achieving a high general level of protection for the environment as a whole.

2.1.1.3 The design helps ensure, for normal operation, compliance with the objectives of optimising occupational exposure to ionising radiation as mentioned in article R. 4451-10 of the Labour Code.

Article R. 4451-10 of the Labour Code
Individual and collective occupational exposure to ionising radiation are maintained below the limits laid down by the provisions of this Title at the lowest level it can reasonably be expected to achieve.

II.1.2 Possible incidents and accidents

Consistently with the provisions mentioned in article 8a introduced by the European Directive of 8th July 2014, the following design objectives are to be adopted:

2.1.2.1 One objective shall be to limit, in the event of incidents or accidents, the releases of radioactive or hazardous substances or the hazardous effects, and their impacts on human and the environment, to levels that are as low as practicable under economically acceptable conditions taking into account progress in the techniques and practices at the time of design. The design objectives in this respect endeavour to ensure continuous improvement in nuclear safety, integrating experience feedback from previous installations.

2.1.2.2 One objective shall be to prevent radiological incidents and accidents and to mitigate the consequences of those that could occur despite the prevention measures adopted; the higher the estimated frequency of the incident or accident, the lower shall be the consequences. To these ends, the design choices shall make it possible to:

- minimise the number of incidents and limit the possibilities of accidents occurring;
- minimise as much as reasonably practicable the frequency of accidents leading to fuel meltdown;
- prevent or, failing this, limit the radioactive releases that can result from incidents or accidents, including accidents with fuel meltdown; provisions aim in particular at preventing contamination of the heat sink and of the groundwater or surface water by radioactive substances.

2.1.2.3 Concerning radiological risks in particular:

- for accidents without fuel meltdown (in the reactor core or pool), the radiological consequences shall be as low as reasonably practicable and, whatever the case, they shall not lead to the need to implement population protection measures (no sheltering, no taking of stable iodine tablets, no evacuation);
- the estimated frequency of fuel meltdown shall be as low as reasonably practicable and, whatever the case, less than 10^{-5} per year and per installation, taking into consideration all types of failures (human, material) and hazards (excluding malicious acts). This estimation shall be supported by uncertainty and sensitivity analyses;
- accident situations with fuel meltdown which could lead to significant radioactive releases that develop too rapidly to allow deployment of the necessary population protection measures in due time shall be rendered physically impossible or, failing this, extremely unlikely with a high degree of confidence
- the population protection measures that would be necessary in the event of the other accidents with fuel meltdown shall be very limited in terms of extent and duration (no permanent relocation, no evacuation outside the immediate vicinity of the site, no sheltering outside the vicinity of the site, no long-term restriction on the consumption of foodstuffs outside the vicinity of the site). To this end, such accidents shall not lead to widespread contamination and long-term pollution of the environmental media.

2.1.2.4 The design helps ensure, for incident and accident conditions, compliance with the objectives of optimising the exposure of workers to ionising radiation as mentioned in article R. 4451-10 of the Labour Code.

II.2 General principles

2.2.1 The general installation design procedure shall be based on a prudent deterministic approach applying the principle of defence in depth supplemented by a probabilistic approach. It necessitates determining the events that could affect a barrier or safety function and then defining the measures to implement on the installation to prevent these events and, if the events are plausible, to limit their consequences.
The design choices shall aim at achieving the safety objectives presented in chapter II.1.2.

II.2.1 Defence in depth

2.2.1.1 The principle of defence in depth mentioned in article 3.1 of the order of 7th February 2012 is applied by implementing successive levels of defence designed to prevent incidents and accidents and, should the prevention measures fail, to limit their consequences:

- The aim of the *first level of defence* is to prevent incidents;
- The aim of the *second level of defence* is to detect the occurrence of such incidents and apply measures that will firstly prevent them from leading to an accident, and secondly restore a situation of normal operation or, failing this, place and maintain the reactor in a safe condition.
- The aim of the *third level of defence* is to control accidents that could not be avoided or, failing this, limit their aggravation by regaining control of the installation in order to return it to and maintain it in a safe condition;
- The aim of the *fourth level of defence* is to manage accident situations resulting from failure of the provisions of the first three levels of defence in depth and leading to fuel meltdown in order to mitigate their consequences, especially for humans and the environment.

Article 3.1 of the order of 7th February 2012

I. - The licensee applies the principle of defence in depth, which consists in deploying successive and sufficiently independent levels of defence aiming, with regard to the licensee, at:

- preventing incidents;
- detecting incidents and applying measures that will firstly prevent them from leading to an accident, and secondly restore a situation of normal operation or, failing this, place and maintain the installation in a safe condition;
- controlling accidents that could not be avoided or, failing this, limit their aggravation by regaining control of the installation in order to return it to and maintain it in a safe condition;
- managing accident situations that could not be controlled so as to mitigate the consequences, especially for humans and the environment.

While the fourth level of defence serves to manage accident situations with fuel meltdown, the third level aims at preventing this meltdown in the design reference envelope (level 3a) and in the design extension envelope (level 3b), which are defined in chapters III.3 and III.4 respectively.

Furthermore, a fifth level of defence in depth targeting emergency management by the public authorities aims at limiting the radiological consequences of radioactive releases that could result from accident conditions. Specific design measures shall be planned for in this respect. This aspect is developed in chapter VII.5.

2.2.1.2 These levels of defence shall be sufficiently independent to meet the objectives specified in chapter II.1.2. Chapter IV.1.2 provides recommendations to this effect.

II.2.2 Barriers

2.2.2.1 With regard to radiological risks, to meet the regulatory requirements set out more specifically in III of article 3.4 and II of article 4.1.1 of the order of 7th February 2012 and in order to prevent or, failing this, limit the dispersion of radioactive substances, the installation features one or more physical barriers placed between these substances and people and the environment.

Article 3.4 of the order of 7th February 2012

III. - The function of radioactive substance containment is ensured by placing one or more successive and sufficiently independent barriers between these substances and people and the environment, and if necessary by a dynamic containment system. The number and effectiveness of these systems are proportional to the potential extent and impact of the radioactive releases, including in the event of an incident or accident.

Article 4.1.1 of the order of 7th February 2012

II. - The licensee takes all necessary measures to avoid unplanned runoffs and discharges into the environment.

2.2.2.2 More specifically, in states in which the reactor primary system is closed, three barriers shall be placed between the fuel pellets loaded in the reactor pressure vessel (RPV) and the environment:

- the 1st barrier made up by the fuel cladding;
- the 2nd barrier made up by the main primary system boundary as defined in the order of 10th November 1999;
- the 3rd barrier which comprises:
  - the reactor containment (reactor building), the containment penetrations and their isolation systems;
  - the boundary of the main secondary systems within the reactor building;
  - the boundary of the systems belonging to the systems whose operation is required during incidents or accidents to fulfil a safety function and carrying radioactive fluid (primary fluid or containment atmosphere) outside the reactor containment.

2.2.2.3 The barriers mentioned in section 2.2.2.1 of this guide are sufficiently mutually independent; more specifically, the design of the installation shall be such that the plausible failure of a barrier does not lead to the failure of a barrier that surrounds it.
Furthermore, their design shall result from a prudent approach, including margins aiming to prevent or delay their failure in normal operation and in incident and accident situations.
The barrier design requirements and the measures taken at the different levels of defence in depth shall enable the functions mentioned in I of article 3.4 of the order of 7th February 2012 to be ensured.

Article 3.4 of the order of 7th February 2012

I. - The demonstration of nuclear safety describes how the following functions are ensured:

- control of nuclear chain reactions;
- evacuation of the thermal power produced by the radioactive substances and nuclear reactions
- containment of radioactive substances;
- protection of people and the environment against ionising radiation.

II.2.3 Functions serving to prevent incidents or accidents or to limit their consequences

2.2.3.1 Pursuant to II of article 3.1 of the order of 7th February 2012, the functions necessary for the demonstration of nuclear safety are identified. With regard to radiological risks, this concerns safety functions and support functions.

Article 3.1 of the order of 7th February 2012

II. - Implementation of the principle of defence in depth is based chiefly on … a cautious design approach, integrating design margins and wherever necessary introducing adequate redundancy, diversification and physical separation of the elements important for protection that fulfil functions necessary for the nuclear safety case, to obtain a high level of reliability and guarantee the functions,…;

2.2.3.2 With regard to radiological risks, design measures shall enable the functions necessary for the demonstration of nuclear safety to be ensured in normal operation and in incident or accident situations. Pursuant to II of article 3.1 of the order of 7th February 2012, these provisions enable a high level of reliability to be obtained for each fundamental function mentioned in I of article 3.4 of the order of 7th February 2012.

II.2.4 Demonstration of nuclear safety - General approach

2.2.4.1 With regard to radiological risks, the demonstration of nuclear safety shall demonstrate that the frequencies of incidents or accidents and their consequences, given the current state of knowledge, practices and the vulnerability of the environment of the installation, are as low as practicable under acceptable economic conditions.
This implies:

- determining the events that can affect the nuclear safety of the installation (single initiating events (SIE), external and internal hazards; see chapters III.1 and III.5) in order to select those to analyse (chapter III.2) by deploying methods in compliance with the principles set out in chapter III.7:
    - the SIEs and the most plausible hazards shall be examined in a **design "reference" envelope** (chapter III.3) in order to determine, on the basis of a conservative approach, the measures to limit their effects;
    - more complex or more severe events (see chapter III.4) than those above shall be examined in a **design "extension" envelope** in order, on the basis of an appropriate procedure, to increase the ability to cope with them;
- performing probabilistic safety assessments (see chapter III.6) in order to consolidate the design choices;
- applying the recommendations given in chapters III to VII to the measures to implement.

III DEMONSTRATION OF NUCLEAR SAFETY

III.1 Identification of events that can affect the nuclear safety of the installation

3.1.1 In order to determine the events to analyse in the demonstration of nuclear safety (see III.2), all the events that can affect the nuclear safety of the installation during normal operation (including reactor outage states) shall be identified on the basis of:

- postulated initiating events (PIE) comprising:
  - the single initiating events (SIE);
  - the internal hazards that can lead directly or indirectly to damage of the EIPs necessary to fulfil the safety functions;
  - the external hazards of natural origin or associated with human activities in the environment of the installation, which can lead directly or indirectly to damage of the EIPs necessary to fulfil the safety functions;
- plausible combinations of initiating events or one initiating event with failure of the measures implemented to cope with it.

Hazards caused by malicious acts are addressed in chapter III.5 of this guide.

III.2 Consideration of events that can affect the nuclear safety of the installation

3.2.1 In the demonstration of nuclear safety, the initiating events are either "excluded" or "postulated".

3.2.2 An initiating event can be "excluded" if it is demonstrated that its occurrence is physically impossible or extremely unlikely with a high degree of confidence with regard to the safety objectives (see II.1). For the SIEs, concrete design and construction measures shall be implemented on the installation, usually supplemented by operating provisions (monitoring and in-service inspection in particular), to justify such an exclusion.
Save exceptions, if an initiating event is excluded, its consequences are not studied.

3.2.3 For the initiating events that are not excluded, their occurrence is postulated and their consequences are assessed. Measures shall be taken to prevent[6] their occurrence and to limit their consequences with a view to achieving the objectives defined in chapter II.1 of this guide.

[6] For external hazards, these prevention measures are based above all on the appropriate choice of the site.

3.2.4 Pursuant to paragraph II of article 3.2 of the order of 7th February 2012, the plausible combinations of initiating events are addressed in the demonstration of nuclear safety.

> **Article 3.2 of the order of 7th February 2012**
>
> II. - In addition to the postulated single initiating events, the demonstration of nuclear safety addresses plausible situations of combined initiating events, selected in accordance with criteria justified notably in the light of the analyses and assessments mentioned in articles 2.7.2 and 3.3.

> **Article 3.3 of the order of 7th February 2012**
>
> The nuclear safety demonstration shall also include probabilistic analyses of accidents and their consequences, unless the licensee demonstrates that this is irrelevant. Unless otherwise specified by ASN, these analyses can be carried out in accordance with methods applied to the installations mentioned in article L. 512-1 of the environment code. They integrate the technical, organisational and human dimensions.

3.2.5 Measures shall be implemented to mitigate the consequences of accidents with core meltdown with a view to achieving the safety objectives mentioned in II.1.

3.2.6 Pursuant to article 3.9 of the order of 7th February 2012, accident situations with fuel meltdown which could lead to significant radioactive releases that develop too rapidly to allow timely deployment of the necessary population protection measures shall be rendered physically impossible or, failing this, measures shall be implemented to render them extremely improbable with a high level of confidence. The justifications for these measures shall be based on a deterministic analysis, consolidated where relevant by probabilistic evaluations, taking account of uncertainties due to the limited knowledge of certain physical phenomena.

Without aiming to be exhaustive, the situations in question can be:

- reactivity accidents which could result from the rapid introduction of cold water or water with a low neutron absorber concentration into the core;
- primary system overpressure accidents which could lead to rupture of the RPV and failure of the reactor containment;
- global or local hydrogen detonations which could lead to failure of the reactor containment;
- steam explosions inside or outside the RPV which could lead to failure of the reactor containment;
- exposure of spent fuel assemblies stored under water or during handling;
- fuel meltdown with containment bypassing;
- core meltdown with a high pressure maintained in the primary system which could lead to bypassing or failure of the reactor containment.

Article 3.9 of the order of 7th February 2012

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.

3.2.7 The probabilistic safety assessments (PSA) mentioned in article 8.1.2 of the order of 7th February 2012 are carried out in order to consolidate the design choices with respect to the objectives mentioned in chapter II.1 of this guide.

Article 8.1.2 of the order of 7th February 2012

For any basic nuclear installation comprising one or more nuclear reactors, the probabilistic analyses mentioned in article 3.3 include probabilistic safety assessments associated with the risk of damaging the nuclear fuel and the risk of abnormal releases of radioactive substances.

III.3 Design reference envelope

The design "reference" envelope comprises the SIEs postulated in the demonstration of nuclear safety, grouped and classified in design-basis condition categories (see chapter III.3.1), and the internal and external hazards taken into consideration, called design-basis hazards (see chapters III.3.2 and III.3.3).
The aim of the safety case for the design reference envelope is to demonstrate, on the basis of a conservative approach, the appropriateness of the measures taken to limit the effects of the SIEs and of the most plausible hazards.
The following paragraphs present the recommendations concerning more specifically the objectives and requirements associated with the analysis of the events considered in the design reference envelope.

III.3.1 Design-basis conditions

III.3.1.1 Events taken into consideration and determination of the design-basis condition categories

3.3.1.1.1 The determination of the design-basis condition categories (DBC) shall result from:
- the identification of the SIEs whose consequences affect at least one safety function;
- the exclusion of the SIEs for which prevention measures are sufficient (see 3.2.2) ;
- the grouping of the non-excluded SIEs to define a limited number of design-basis conditions for which the consequences encompass those of the events of the corresponding group.

3.3.1.1.2 The SIEs addressed in the demonstration of nuclear safety shall essentially be defined on a deterministic basis taking into account in particular the specificities of the design of the installation in question, the different operating states of the installation and the experience with reactors, whether similar or not, in France or abroad, in operation or under construction.
For the reactor or the fuel storage pool, the SIEs to consider are those that lead to an abnormal change in at least one parameter that is characteristic of the fulfilment of a safety function.

The SIEs can lead to:
- excessive cooling or heating of the primary cooling system water;
- a reduction in the primary cooling system water flow rate;
- a loss of water inventory or an uncontrolled water input into the primary cooling system;
- an uncontrolled change in the nuclear chain reactions;
- an uncontrolled increase or decrease in the primary cooling system pressure;
- loss of cooling of the fuel assembly storage pool;
- a reduction in the quantity of water present in a compartment of a pool containing one or more fuel assemblies;
- abnormal dissemination of radionuclides (for example by rupture or loss of sealing of components containing radioactive substances, or by deterioration of fuel assemblies during a handling operation).

3.3.1.1.3 The design-basis conditions shall be classified in categories. Their allocation to the different categories shall be carried out primarily according to the estimated frequencies of occurrence of the corresponding SIE groups.
The design-basis conditions are thus classified in four categories:
- normal operation (category 1 or DBC-1), where the installation is maintained within the limits defined by its operating technical specifications;
- incidents (category 2 or DBC-2) with an estimated annual occurrence frequency per reactor higher than 10^{-2};
- accidents of category 3 (or DBC-3) with an estimated annual occurrence frequency per reactor higher than 10^{-4} and lower than 10^{-2};
- accidents of category 4 (or DBC-4) with an estimated annual occurrence frequency per reactor lower than 10^{-4} and which were not excluded under article 3.2.2. Implausible combinations of accident and initial state can, subject to suitable justification, not be postulated.

3.3.1.1.4 Particular attention shall be paid to:

- the outage states presenting specific conditions, particularly when certain EIPs or containment barriers are not available (for example during opening of the main primary system, opening of the air lock or the reactor containment equipment access hatch) or when workers can be present inside the reactor containment;
- the events that can affect the fuel stored in the pool and those that can affect the fuel in the RPV and the fuel stored in the pool simultaneously;
- the events that could lead to bypassing of the reactor containment.

III.3.1.2 Objectives and requirements associated with the design-basis conditions

3.3.1.2.1 For each category of design-basis conditions, objectives shall be defined in terms of confinement barriers resistance, heat removal and control of reactivity.

3.3.1.2.2 Requirements, resulting in particular from the abovementioned objectives, shall be defined by the applicants for each design-basis conditions category. These requirements shall be associated with the various physical phenomena that could go against these objectives.
The higher the estimated frequency of the corresponding design-basis condition, the more stringent shall be the objectives and requirements set by the applicants.

3.3.1.2.3 For all the design-basis conditions in categories 2 to 4:

- a design-basis condition shall not in itself cause loss of a function intended to limit the consequences of that condition;
- the measures taken with respect to the control of nuclear chain reactions:
  - aim at avoiding reaching critical conditions in situations where the reactor is already shut down when the SIE occurs;
  - shall guarantee the absence of criticality in the fuel assembly storage pool;
- core cooling shall be ensured. This more specifically necessitates maintaining a geometry that can be cooled;
- when in a design-basis condition, the installation shall reach a controlled state and be brought to, then maintained in, a safe state[7] under the following conditions:
  - achieving the controlled state does not require manual operator action unless specifically justified;
  - the controlled state implies a water inventory that is stable, or even increasing (in the primary cooling system and in the pools) and without exposure of fuel assemblies (for the fuel assembly storage pool);
  - achieving the safe state does not necessitate any human action in the short term (see 3.3.1.4.5) ;
  - in the event of emptying of the fuel assembly storage pool, the safe state implies that emptying stops before any fuel assemblies become uncovered;
  - in safe state, achieving conditions that enable heat to be removed by the main heat sink is a priority;
- the cooling and confinement of the fuel assemblies stored or handled in pools shall be ensured. More specifically, the fuel assemblies shall remain under water and any radioactive discharges shall be filtered (see article 6.3.1.3);
- a design-basis condition shall not lead to dispersion in the primary system of a quantity of fuel pellets or fragments of pellets that produces a significant effect. If the reactor can be operated with a few cladding defects and it cannot be demonstrated that there is no dispersion of fuel in the primary cooling system, the absence of significant consequences in the event of dispersion shall be demonstrated.

3.3.1.2.4 The category-1 and -2 design-basis conditions shall not lead to loss of integrity[8] of a confinement barrier.

More specifically, integrity of the fuel rods with respect to the different damage modes[9] shall be demonstrated: the various physical phenomena (hydraulic, thermohydraulic, mechanical and thermal) loading the first confinement barrier shall be taken into account.

[7] See appendix 1 for the definitions of "safe state" and "controlled state".

[8] The controlled opening or momentary opening of a valve is not considered as constituting a loss of integrity if the opening is considered in the nuclear safety case.

[9] They include in particular wear and fatigue (in category 1), the pellet-cladding interactions and the consequences of the boiling crisis (in categories 1 and 2).

3.3.1.2.5 A category-2 or -3 design-basis condition shall not cause a design-basis condition of a higher category.

3.3.1.2.6 For category-3 accidents:
- melting of the fuel pellet at the core hot spot shall be avoided;
- the damage suffered by the fuel assembly structure and the fuel rods shall not call into question the possibility of unloading and storing the fuel;
- the main primary system shall not suffer damage affecting its integrity other than the direct consequences of the SIE;
- the integrity of the reactor containment shall be ensured and the other components of the 3rd barrier shall not suffer damage affecting their integrity other than the direct consequences of the SIE.

3.3.1.2.7 For category-4 accidents:
- melting of the fuel pellet at the core hot spot shall remain limited;
- the main primary system shall not suffer damage affecting its integrity other than the direct consequences of the SIE;
- the integrity of the reactor containment shall be ensured and the other components of the 3rd barrier shall not suffer damage affecting their integrity other than the direct consequences of the SIE.

3.3.1.2.8 In order to limit the radiological consequences of category-3 and -4 accidents, damage to the 1st barrier shall be limited in terms of the number of fuel rods affected and damage severity. The damage shall be less severe for category-3 accidents than for category-4 accidents.

III.3.1.3 Technical acceptance criteria associated with the design-basis conditions

3.3.1.3.1 In practice, the technical acceptance criteria shall be defined in order to produce an operational breakdown of the objectives and requirements mentioned in chapter III.3.1.2 of this guide.
The higher the estimated frequency of the corresponding design-basis conditions category, the more severe shall be the criteria.
These criteria can incorporate conservative simplifications or margins with respect to the requirements.

3.3.1.3.2 The technical acceptance criteria shall focus on representative quantities of restrictive physical phenomena, accessible by calculation or measurable on the installation. The limit values shall be determined as far as practicable on the basis of representative experiments of situations encountered under the design-basis conditions.

3.3.1.3.3 The technical acceptance criteria relative to the behaviour of the fuel shall focus in particular on the maximum temperature of the fuel pellets, on the critical thermal flux ratio, on the mechanical resistance of the fuel cladding, on the temperature of the cladding and its level of oxidation or hydride content, and on the maximum fraction of fuel rods with damaged cladding.

3.3.1.3.4 Compliance with the technical acceptance criteria shall be verified by analyses of the design-basis conditions.

3.3.1.3.5 For the SIEs involving steam generator tube rupture considered in the design reference envelope, releases of liquid water from the primary cooling system into the environment shall be avoided as much as reasonably practicable.

III.3.1.4 Analysis rule for design-basis conditions

3.3.1.4.1 The design-basis condition analyses shall follow analysis rules and take into account the state of the installation as it is known or can be predicted, particularly in view of operating experience feedback from similar installations.
These rules shall ensure the conservative nature of the design-basis condition analyses (see III.7). Adopting "conservative" assumptions[10] represents good practice in this respect

3.3.1.4.2 The analysis rules for category-2 to -4 design-basis conditions shall more specifically define the procedures relative to:

- the initial conditions and the limit conditions taking into account the normal planned operating envelope of the installation and a fuel state that is compatible with this normal operation;
- the operator actions (see 3.3.1.4.5);
- the failure to postulate with respect to the aggravating factor (see 3.3.1.4.4);
- application of the addition of a loss of off-site electrical power supply to these design-basis conditions (see 3.3.1.4.6);
- to the controlled and safe states for the installation (see 3.3.1.2.3);
- to the EIPs and other equipment concerned, such as the installation regulating equipment (cf. 3.3.1.4.3);
- the unavailability of required EIPs, in view of the preventive maintenance programmes.

[10] With regard to the pellet and cladding interaction, reasonably conservative analysis rules adapted to the nature of the risk are considered.

3.3.1.4.3 In the category-2 to -4 design-basis condition analyses:

- the EIPs that have an appropriate classification (as defined in chapter IV.2.1 of this guide) can be taken into account;
- the EIPs taken into account in the demonstration of nuclear safety are assumed to function correctly at their level of performance which is on the whole the most penalizing with respect to the technical acceptance criteria for the design-basis condition;
- the systems, structures and components (SSC) which are not EIPs or do not have an appropriate classification (as defined in IV.2.1):
    - shall be taken into consideration if their normal operation penalises compliance with the technical acceptance criteria associated with the design-basis condition;
    - can be taken into consideration for their favourable effect, provided that proof of their ability to function under the environmental conditions associated with the DBC condition for the required duration, if they are in service before occurrence of the initiating event and remain in operation, under the same conditions as those preceding occurrence of the initiating event (no change of state, no change of operating or environmental parameters). It shall be verified that the failure to consider these SSCs in the demonstration of nuclear safety is covered in terms of consequences by another design-basis condition which can be of the same or a higher category;
    - can, exceptionally, be taken into consideration for their favourable effect with respect to compliance with the technical acceptance criteria associated with the design-basis condition, subject to the application of appropriate requirements. It shall be verified that the failure to consider these SSCs in the demonstration of nuclear safety is covered in terms of consequences by another design-basis condition which can be of the same or a higher category;
- the regulation functions which, in application of the general rule are not taken into account, are assumed to leave the equipment items they control in the position they were in at the initial moment.

3.3.1.4.4 The analyses of the category-2 to -4 design-basis conditions shall consider the most penalising aggravating failure with respect to the required technical acceptance criteria. The failures to consider as aggravating failure shall take into account the recommendations given in chapter IV.2.3[11]. More specifically, jamming of the most anti-reactive control rod cluster is a potential aggravating failure.
The failure taken as the aggravating failure does not change the category of the analysed design-basis condition.

3.3.1.4.5 Under the analysis rules for the design-basis conditions in categories 2 to 4, a minimum time frame shall be adopted for performing the first manual action after sending the first significant information to the operators following the SIE:

- 30 minutes for action initiated from the main control room;
- one hour for action outside the main control room.

Particular cases corresponding to operating phases where presence of personnel outside the control room is mandatory may be accepted subject to justification.

[11] The failures induced by the SIE are not considered as aggravating factors because they are considered to be consequences of the SIE.

Furthermore, the feasibility of the human actions necessary to bring the reactor to and maintain it in a safe state shall be ensured.

3.3.1.4.6 It is considered that an earthquake can cause loss of the off-site electrical power supplies and induce a design-basis condition. A good design practice is to analyse all the design-basis conditions (apart from those that would result from human action) by postulating the combination of loss of off-site electrical power with the design-basis condition, and this at the least favourable moment. As a minimum, the following moments are considered: initiating moment, reactor automatic shutdown signal, signal to inject emergency water into the core.
In the analyses that consider this combination:

- only the EIPs that remain operational during or after an earthquake can be used in the demonstration of nuclear safety;
- a rod drop time that is longer than that used in the analysis without taking the earthquake into account is adopted;
- the technical acceptance criteria to satisfy are those of the category-4 design-basis conditions.

III.3.1.5 Assessment of the radiological consequences of the design-basis conditions

3.3.1.5.1 The radiological consequences of the design-basis conditions are assessed in accordance with the provisions of article 3.7 of the order of 7th February 2012 and article 4.7.1 of ASN resolution 2015-DC-532 of 17th November 2015 relative to the safety analysis report of basic nuclear installations.

Article 3.7 of the order of 7th February 2012

I. - The demonstration of nuclear safety includes an assessment of the potential consequences, radiological or not, of the envisaged incidents and accidents. For each scenario, this assessment includes:

- a presentation of the assumptions used in the release calculations and exposure scenarios; the release calculation assumptions must be reasonably pessimistic and the exposure scenarios must be based on realistic parameters, but without considering any population protection actions that could be implemented by the public authorities;
- an estimation of the effective doses and the intensity of the non-radiological phenomena to which persons and the environment could be exposed in the short, medium and long term, distinguishing the different age classes where necessary, and considering the different hazardous substance transfer pathways; the estimation includes equivalent doses to the thyroid in the event of radioactive substance releases that justify this;
- an estimation of the extent of the areas likely to be affected;
- for incidents or accidents having consequences outside the site, the kinetics of the development of the hazardous phenomena and the propagation of their effects.

…

III. - The intensity of the hazardous radiological phenomena is defined with respect to reference values expressed as levels of intervention of the public authorities in radiological emergency situations, as defined by the ASN in application of article R. 1333-80 of the Public Health Code.

Article 4.7.1 of ASN Resolution 2015-DC-0532 of 17th November 2015 relative to the safety analysis report for basic nuclear installations

For the application of article 3.7 of the abovementioned order of 7th February 2012, the safety analysis report sets out the potential consequences, radiological or not, of the incidents and accidents, with the exception of the accidents mentioned in article 4.4.9 of this appendix. The safety analysis report specifies the following points in particular:

- the hypotheses, rules and methods used to make the evaluation,
- in the case of radiological releases, a description of the physical-chemical form of the released radionuclides contributing the most to the consequences of the releases,
- for incidents or accidents resulting in hazardous or radioactive substances being released into the environment, the direct consequences of the release phase, chiefly associated with atmospheric releases and possible direct releases in the ground and the aquatic environment ,
- for the most representative accidents leading to radioactive releases, the evaluation as a function of time:
    - of the consequences associated with the releases in terms of surface activity and possibly ambient dose rate,
    - of the mass contamination of agricultural commodities and, if applicable, the contamination of water resources.

3.3.1.5.2 Concerning the design-basis conditions for which only release calculations are performed, such as the break of radioactive effluent tanks or a fuel element handling accident, an aggravating failure affecting the radioactive substance containment safety function shall be adopted.

3.3.1.5.3 The assessment of the radiological consequences of events in the design reference envelope contributes to the verification of the adequacy of the design provisions adopted with respect to the safety objectives mentioned in chapter II.1 of this guide. Criteria for assessing the consequences for humans and the environment and enabling these objectives to be satisfied shall be defined for each design-basis conditions category.

III.3.2 Design-basis internal hazards (excluding malicious acts)

III.3.2.1 Design objectives and principles associated with the design-basis internal hazards

3.3.2.1.1 Defence in depth applied to protection against the design-basis internal hazards aims at limiting their occurrence and consequences by putting in place concrete measures.

3.3.2.1.2 For each design-basis internal hazard, measures shall be implemented to:

- limit their occurrence;
- detect their occurrence when necessary;
- guarantee the availability of a set of EIPs that can fulfil the safety functions despite all the effects (direct and indirect) of the internal hazard in question, considering the analysis rules for that hazard (see chapter III.3.2.3);
- enable a safe state to be reached and maintained;
- avoid calling into question the justifications for excluding the initiating events mentioned in article 3.2.2.

More specifically, the buildings housing EIPs necessary to bring the reactor to, and maintain it in, a safe state and the buildings containing significant quantities of radioactive substances shall be designed taking the internal hazards into consideration.

3.3.2.1.3 The design of the fire-risk control provisions meet the regulatory requirements of ASN resolution 2014-DC-0417 of 28th January 2014 concerning the rules applicable to basic nuclear installations (BNI) with regard to the control of fire risks.

Article 1.2.1 of ASN resolution 2014-DC-0417 of 28th January 2014 concerning the rules applicable to basic nuclear installations (BNI) with regard to control of fire risks

Pursuant to Article 3.1 of the above-mentioned order of 7th February 2012, the licensee applies the principle of defence in depth to the control of fire risks.

The licensee thus implements successive and sufficiently independent levels of defence designed to protect or perform the functions defined in Article 3.4 of the above-mentioned order of 7th February 2012.

These levels are based in particular on:

- preventing the outbreak of fire;
- detecting and rapidly extinguishing any outbreaks, on the one hand to prevent them leading to a fire and, on the other, to restore a normal operating situation or, failing this, attain then maintain a safe BNI state;
- mitigating the aggravation and propagation of a fire which have not been stopped, in order to minimise its impact on nuclear safety and enable a safe BNI state to be attained or maintained;
- the management of accident situations resulting from a fire which could not be stopped, in order to mitigate the consequences for individuals and the environment.

3.3.2.1.4 A design-basis internal hazard should not lead to an accident[12].

3.3.2.1.5 In application of II of article 3.1 of the order of 7th February 2012, the risks of common mode failures due to design-basis internal hazards shall be considered and, if necessary, physical or geographical separations shall be provided for between the redundant parts of systems fulfilling a safety function.

III.3.2.2 Events considered as design-basis internal hazards

3.3.2.2.1 The design-basis internal hazards to be considered in the demonstration of nuclear safety are those mentioned in article 3.5 or the order of 7th February 2012. Hazards associated with malicious acts are addressed in chapter III.5 of this guide.

Article 3.5 of the order of 7th February 2012

The internal hazards to be considered in the demonstration of nuclear safety include:

- Projections of projectiles, notably those resulting from the failure of rotating equipment;
- pressure equipment failures;
- load collisions, falling loads;
- explosions;
- fires;
- hazardous substance emissions;
- floods originating within the perimeter of the basic nuclear installation;
- electromagnetic interference;
- malicious acts;
- any other internal hazard identified by the licensee or that ASN considers must be taken into consideration;
- plausible combinations of the above hazards.

[12] Nevertheless, some initiating events in themselves constitute both an internal hazard and an accident (break of a pipe, for example).

3.3.2.2.2 The plausible combinations of design-basis internal hazards are taken into consideration; they shall take account of any interdependencies between the initiating events.

3.3.2.2.3 The design-basis internal hazards shall, depending on their plausibility, be taken into account during the long-term phase of design-basis conditions after reaching the safe state. In this case of a conventional combination, the failure postulated on account of the aggravating failure and the combination of a loss of off-site electrical power are not applied.

III.3.2.3 Analysis rules for design-basis internal hazards

3.3.2.3.1 The analysis of the design-basis internal hazards shall follow analysis rules appropriate for the hazard and take into account the state of the installation such as it is known or can be predicted, particularly in view of operating experience feedback from similar installations.

The analysis rules for design-basis internal hazards shall in particular define the way in which the following are taken into account:

- the initial conditions taking account of the normal planned operating range of the installation;
- the operator actions,
- the targeted safe states for the installation;
- EIPs and other installation equipment items concerned, given their classification;
- the unavailability of required EIPs, in view of the preventive maintenance programmes.

The design-basis internal hazard analyses shall consider the most penalising aggravating failure with respect to the targeted safe state. The failures to be envisaged as aggravating failures shall take into account the recommendations given in chapter IV.2.3. The conditions that, where applicable, enable the failure of certain EIPs not to be considered as aggravating failures shall be substantiated. This can be the case for passive components IP if their failure is highly improbable.

3.3.2.3.2 The analysis of a design-basis internal hazard shall be carried out:

- assuming the failure of all the EIPs that could be affected by the hazard or its consequences and which are neither robust to this hazard or its consequences nor protected against this hazard or its consequences, if their failure is penalising;
- taking into account the feasibility of the human actions to perform in view of the hazard and its consequences;
- by analysing all the direct and indirect effects induced by this hazard, including those that are induced by the measures implemented to deal with this hazard.

3.3.2.3.3 The consequences of the design-basis internal hazards shall be examined in all the normal operating states of the reactor, including the outage states, taking account of the specific configurations encountered in these states. Implausible combinations of internal hazards and initial conditions can, subject to justification, be ignored.

III.3.2.4 Assessment of the radiological consequences of the design-basis internal hazards

3.3.2.4.1 If a design-basis internal hazard leads to radioactive releases, the associated radiological consequences are assessed in accordance with the provisions of article 3.7 of the order of 7th February 2012 and article 4.7.1 of ASN resolution 2015-DC-0532 of 17th November 2015 relative to the safety analysis report of basic nuclear installations. The method of assessing the radiological consequences shall be similar to that used for assessing the radiological consequences of the design-basis conditions.

3.3.2.4.2 The assessment of the radiological consequences of design-basis internal hazards contributes to the verification of the adequacy of the design provisions adopted with respect to the safety objectives mentioned in chapter II.1 of this guide. The criteria for assessing the radiological consequences of the situations resulting from a design-basis internal hazard shall be the same as those mentioned in 3.3.1.5.3 for the category of design-basis conditions with an equivalent frequency of occurrence.

III.3.3 Design-basis external hazards (excluding malicious acts)

III.3.3.1 Design objectives and principles associated with the design-basis external hazards

3.3.3.1.1 For each design-basis external hazard, measures shall be implemented to:

- guarantee the availability of a set of EIPs that can fulfil the safety functions despite all the effects (direct and indirect) of the external hazard in question, considering the analysis rules for that hazard (see chapter III.3.3.3);
- avoid calling into question the justifications for excluding the initiating events mentioned in article 3.2.2.
- enable a safe state to be reached and maintained.

More specifically, the buildings housing EIPs necessary to bring the reactor to, and maintain it in, a safe state, and the buildings containing significant quantities of radioactive substances shall be designed taking the external hazards into consideration.

3.3.3.1.2 The measures taken with regard to external hazards shall be based in priority on static systems. Measures shall be implemented where relevant to give the alert and monitor the development of an external hazard (particularly for foreseeable external hazards).

3.3.3.1.3 The measures taken with respect to the design-basis external hazards shall not call into question the protection against the other events in the design reference envelope.

3.3.2.1.4 A design-basis external hazard should not lead to an accident[13].
Moreover, the systems IP fulfilling safety functions under DBC-3 and 4 conditions shall remain capable of fulfilling these functions after a reference earthquake and design-basis external flooding.

[13] The particular case of loss of off-site electrical power induced by an earthquake is addressed in paragraph 3.3.1.4.6.

A good practice consists in ensuring that the systems IP fulfilling safety functions under DBC-3 and DBC-4 conditions remain capable of fulfilling these functions after a design-basis external hazard, and even during it when appropriate.

3.3.3.1.5 The analysis of design-basis external hazards shall include the following five steps:

- selection of the external hazards relevant for the installation;
- characterisation of the selected design-basis external hazards;
- defining of the procedures for taking design-basis external hazards into account for the nuclear installation;
- determination of the EIPs whose function shall continue to be ensured during or after the selected external hazards;
- demonstration of the adequacy of the measures taken with respect to the selected external hazards.

III.3.3.2 Events considered as design-basis external hazards and their characterisation

3.3.3.2.1 The external hazards are linked to the site on which the installation is located and can affect consecutively or simultaneously all or part of the installations on the site. Consequently, in accordance with the provisions of the second paragraph of II of article 3.1 of the order of 7th February 2012, particular attention is made to the choice of site.

Article 3.1 of the order of 7th February 2012

II. - Application of the principle of defence in depth is based chiefly on:
- the choice of an appropriate site, with particular consideration for the natural or industrial risks weighing on the installation;

3.3.2.2.1 The design-basis external hazards to take into consideration in the demonstration of nuclear safety are those mentioned in article 3.6 or the order of 7th February 2012. Hazards associated with malicious acts are addressed in chapter III.5 of this guide.

Article 3.6 of the order of 7th February 2012

The external hazards to be considered in the demonstration of nuclear safety include:
- the risks induced by industrial activities and communication routes, including explosions, hazardous substance emissions and airplane crashes;
- earthquake;
- lightning and electromagnetic interference;
- extreme meteorological or climatic conditions;
- fires;
- floods originating outside the perimeter of the basic nuclear installation, including their dynamic effect;
- malevolent acts;
- any other external hazard identified by the licensee or that ASN considers must be taken into consideration;
- plausible combinations of the above hazards.

3.3.3.2.3 An external hazard among those in the list mentioned in article 3.6 of the order of 7th February 2012 can only be excluded on the basis of a justification based on a conservative approach which concludes, with a high degree of confidence, either that the hazard cannot affect the installation or that the frequency of occurrence of the hazard is extremely low.

3.3.3.2.4 The plausible combinations of design-basis external hazards are taken into consideration; they shall in particular take account of any interdependencies between the initiating events.
Particular attention shall be paid to external hazards that have a common origin[14].

3.3.3.2.5 The selection and characterisation of the chosen design-basis external hazards shall include more specifically:

- the available data concerning the reactor site and its natural and industrial environment, particularly the data resulting from measurements or based on reported or observed historical events;
- the foreseeable developments of these hazards during the service life of the reactor, particularly those concerning climatic conditions and meteorology.

3.3.3.2.6 The design-basis external hazards adopted in application of articles 3.3.3.2.2 and 3.3.3.2.3 of this guide shall be characterised using deterministic methods and, when possible and relevant, probabilistic methods.
These methods shall take into consideration all the available data and, when possible, enable a relationship to be established between the severity of the external hazard and its annual exceedance frequency[15]. They also satisfy the characteristics set in I of article 3.8 of the order of 7th February 2012.

Article 3.8 of the order of 7th February 2012

I. - The demonstration of nuclear safety is based on…
- appropriate, clearly explained and validated methods, integrating assumptions and rules adapted to the uncertainties and limits of knowledge of the phenomena in play;

3.3.3.2.7 To determine the hazard levels to consider for the design-basis natural external hazards, a value of 10^{-4}/year for the annual exceedance frequency of the hazard in question shall be targeted.
Nevertheless, for certain design-basis natural external hazards, when the annual exceedance frequency of the hazard cannot be calculated, or if the uncertainties concerning the value are too high, an "event"[16] shall still be considered and justified by aiming for an equivalent objective to that to be targeted in application of the preceding paragraph.

3.3.3.2.8 The hazard or "events" levels considered for the characterisation of design-basis external hazards shall be justified. More specifically, their severity shall be increased with respect to that of the relevant historic "events".

3.3.3.2.9 For the earthquake to consider in the design reference envelope, the maximum ground acceleration shall not be less than 0.1 g at infinite frequency (where "g" is the acceleration due to gravity on the surface of the Earth).

[14] To give an example, ASN Guide No. 13 on the protection of basic nuclear installations against external flooding mentions in article 2.3.2 that "*Combinations of events have been chosen inter alia particular where there is a proven or presumed dependency between events likely to cause flooding.*"

[15] To way of illustration, the flow rate of the watercourse and its annual exceedance frequency.

[16] By way of illustration, taking the hundred-year rainfall events and unavailability of the local stormwater drainage system into consideration can help define such an "event"

III.3.3.1 Analysis rules for design-basis external hazards

As a general rule, the procedure for protecting against design-basis external hazards consists in detailing the "load cases" to be considered for each external hazard and then sizing or protecting the structures and equipment items that shall withstand these load cases accordingly. The aim is to decouple the hazard itself from any induced events.
When such decoupling is not possible or is not aimed for, analyses are carried out in accordance with the rules described below to ensure that the objectives are ultimately satisfied.

3.3.3.3.1 The analyses of the design-basis external hazards shall follow analysis rules appropriate for the hazard and take into account the state of the installation and its site such as they are known or can be predicted.

The analysis rules for design-basis external hazards shall in particular define the way in which the following are taken into account:

- the initial conditions taking account of the normal planned operating range of the installation;
- the operator actions,
- the targeted safe states for the installation;
- EIPs and other installation equipment items concerned in view of their classification;
- the unavailability of required EIPs, in view of the preventive maintenance programmes.

The design-basis external hazard analyses shall consider the most penalising aggravating failures with respect to the targeted safe state. The failures to be envisaged as aggravating failures shall take into account the recommendations given in chapter IV.2.3. The conditions that, where applicable, enable the failure of certain EIPs not to be considered as aggravating failures, shall be substantiated. This can be the case for passive components IP if their failure is highly improbable.

3.3.3.3.2 The analysis of a design-basis external hazard shall:

- consider all the direct and indirect effects induced by this hazard and by the measures implemented to deal with it;
- assuming the failure of all the EIPs that could be affected by the hazard or its consequences and which are neither robust to this hazard or its consequences nor protected against this hazard or its consequences, if their failure is penalising;
- take into consideration the loadings established on the basis of a conservative procedure;
- take account of the fact that an external hazard can simultaneously affect several train of systems IP, several levels of defence in depth, several installations on the site, or even regional infrastructures around the site. In this respect, particular attentions shall be focused on the risk of isolation of the site (accessibility, electrical power networks and communication networks, etc.) and its consequences, particularly in terms of operational control of the installations;
- take into account the feasibility of the human actions to perform in view of the hazard and its consequences;
- take into account, where applicable, the predictability and the kinetics of the hazard.

3.3.3.3.3 The consequences of the design-basis external hazards shall be examined in all the normal operating states of the reactor, including outage states, taking account of the specific configurations

encountered in these states. Implausible combinations of external hazards and initial conditions can, subject to justification, be ignored.

III.3.3.2 Assessment of the radiological consequences of the design-basis external hazards

3.3.2.4.1 If a design-basis external hazard leads to radioactive releases, the associated radiological consequences are assessed in accordance with the provisions of article 3.7 of the order of 7th February 2012 and article 4.7.1 of ASN resolution 2015-DC-0532 of 17th November 2015 relative to the safety analysis report of basic nuclear installations. The method of assessing the radiological consequences shall be similar to that used for assessing the radiological consequences of the design-basis conditions.

3.3.3.4.2 The assessment of the radiological consequences of design-basis external hazards contributes to the verification of the adequacy of the design provisions adopted with respect to the safety objectives mentioned in chapter II.1 of this guide. The criteria for assessing the radiological consequences of the situations resulting from a design-basis external hazard shall be the same as those mentioned in 3.3.1.5.3 for the category-4 design-basis conditions.

III.4 Design extension envelope

With a view to achieving the objectives set out in chapter II.1.2, measures are implemented to:

- ensure that the installation can cope with initiating events that are more complex or more severe than those considered in the design reference envelope;
- limit releases of radioactive substances into the environment during these events.

The situations that result from these events constitute the design extension envelope.

III.4.1 Events considered in the design extension envelope and objectives

3.4.1.1 The list of events to consider in the design extension envelope shall be based on deterministic and probabilistic considerations, consolidated by expert judgment if necessary.
The events in the design extension envelope shall consider:

- conditions termed "DEC-A" for which fuel meltdown shall be prevented. They consider, in principle, with respect to the fuel meltdown frequency objective:
  - combinations of a DBC condition and a common cause failure affecting the redundant parts of an system IP necessary for the control of this DBC condition;
  - common cause failures on the systems IP used in normal operation.

  The probabilistic analyses enable the list of DEC-A conditions (see article 6.3.1) to be confirmed and supplemented if necessary;

- conditions termed "DEC-B" in which fuel meltdown is postulated despite the measures taken to prevent this. The situations mentioned in article 3.2.6 are not included in the design extension envelope;
- natural external hazards of greater severity than those considered in the design reference envelope (see chapter III.4.6 for the corresponding particularities).

3.4.1.2 Consideration of these events aims at:
- for DEC-A conditions, demonstrating the ability of the installation to prevent fuel meltdown in plausible complex accident sequences. It serves to identify, if necessary, the measures that shall be taken to prevent accidents involving fuel meltdown, in addition to the measures identified further to the analysis of initiating events in the design reference envelope;
- for the DEC-B conditions, defining measures aiming to limit the extent and duration of the consequences of accidents involving fuel meltdown;
- for the natural external hazards of greater severity than those considered in the design reference envelope, to check that sufficient margins exist to achieve the objectives set in 2.1.2.3.

3.4.1.3 When appropriate, all the reactors and fuel assembly storage pools on the site shall be considered as being in the design extension conditions.

3.4.1.4 In order to determine the DEC-A conditions, the plausible long-term situations affecting the electrical power supplies or residual heat removal to the heat sink shall in particular be duly examined.

III.4.2 Requirements associated with the DEC-A and DEC-B conditions

3.4.2.1 When a DEC-A condition arises, the installation shall be brought to and maintained in a safe state.

3.4.2.2 The requirements that the applicants set for the DEC-A conditions shall be such that:
- reactivity is controlled; core sub-criticality is ensured after activating the measures mentioned in article 3.4.1.2 and is maintained over the long term;
- the residual heat removal is ensured. More specifically, the residual heat removal from the fuel assembly storage pool by boiling can be tolerated temporarily while the cooling resources causing the DEC-A condition are out of service if a sufficient level of water (see chapter VII.3.3) is maintained in the pool;
- the confinement of radioactive substances is ensured such that the safety objectives set out in chapter II.1.2 applicable to accidents without fuel meltdown are satisfied.

3.4.2.3 When a DEC-B condition arises, the reactor shall be brought to and lastingly maintained in a safe state in which:

- sub-criticality is ensured;
- residual heat removal is ensured, and more specifically the corium is cooled;
- radioactive substances are confined.

3.4.2.4 The requirements that the applicants set for the DEC-B conditions shall be such that:

- confinement of radioactive substances is ensured such that the safety objectives set out in chapter II.1.2 applicable to accidents with fuel meltdown are satisfied (also see chapter III.4.5);
- corium sub-criticality and residual heat removal are ensured over the long term. Nevertheless:
    - subcriticality of the corium may temporarily not be ensured provided that this does jeopardise residual heat removal;
    - the residual heat may temporarily not be evacuated if this does not jeopardise control of the containment of radiological substances; this shall lead in particular to design requirements for the 3rd confinement barrier.

3.4.2.5 The design of measures to limit the consequences of accidents with fuel meltdown shall be underpinned by the state-of-the-art in terms of understanding and modelling accidents with fuel meltdown and by appropriate research and development work (specific tests, simulation tools, etc.).
It shall take into consideration the uncertainties concerning certain phenomena and their modelling.

III.4.3 Technical acceptance criteria associated with the design extension envelope

3.3.1.3.1 Technical acceptance criteria shall be defined for the analysis of the design extension envelope events in order to produce an operational breakdown of the objectives and requirements mentioned in chapter III.4.1 and III.4.2 of this guide. They can be adapted with respect to those adopted for the analyses of the design reference envelope.

III.4.4 Analysis Rules within the design extension envelope

3.4.4.1 The rules and methods for analysing the design extension envelope events can be adapted with respect to those which are adopted for the analysis of the design-basis conditions in order to be less conservative, for example by not taking aggravating failures into consideration or by adopting less "conservative" assumptions.

3.4.4.2 The analysis of events in the design extension envelope shall take into consideration:

- the environment of the installation and its location;
- the ability of the EIPs to fulfil their missions given the conditions encountered in the analysed situations;
- the feasibility of the actions planned in the management of the analysed situations, taking into account the times required to deploy any mobile equipment present on the site or not;
- the contributions of the probabilistic safety analyses.

III.4.5 Assessment of the radiological consequences in the design extension envelope

3.4.5.1 The radiological consequences of events - including hazards - in the design extension envelope are assessed in accordance with the provisions of article 3.7 of the order of 7th February 2012 and article 4.7.1 of ASN resolution 2015-DC-0532 of 17th November 2015 relative to the safety analysis report of basic nuclear installations.

3.4.5.2 The assessment of the radiological consequences of events in the design extension envelope contributes to the verification of the adequacy of the design provisions adopted with respect to the safety objectives mentioned in chapter II.1 of this guide.

III.4.6 Natural external hazards

The following articles provide more details concerning the objectives, requirements, events to consider and rules for the analysis of natural external hazards in the design extension envelope. They result in particular from the lessons drawn from the Fukushima Dai-ichi accident and from the stress tests.

3.4.6.1 Taking natural external hazards into account in the design extension envelope is in line with the objective of minimising the risks described in article 2.1.2.3, as much for the prevention of fuel meltdown as for limiting the population protection measures that would be necessary in the event of accidents involving fuel meltdown.

Consequently, for the natural external hazards in the design extension envelope:

- the safety functions for preventing fuel meltdown in the fuel pool shall continue to be ensured;
- the safety functions for preventing core meltdown should be maintained and, whatever the case, the functions for managing the effects of core meltdown shall continue to be ensured;
- the justifications for excluding the initiating events mentioned in article 3.2.2 shall not be called into question.

3.4.6.2 To identify the natural external hazards to consider in the design extension envelope, the severity of the hazard as a function of its annual exceedance frequency shall be established[17] when this is possible.

Concerning natural external hazards whose annual risk exceedance frequency cannot be calculated, or when the uncertainties concerning this value are too high, an "event" of greater severity than that considered in the design reference envelope shall nevertheless be considered and justified.

3.4.6.3 The design of the EIPs necessary to cope with natural external hazards in the design extension envelope shall be carried out in accordance with the appropriate codified design and construction rules or, failing this, in accordance with the rules of good engineering practice. The provisions of article 4.2.1.10 are applicable.

[17] The hazard level whose exceedance is extremely improbable with a high level of confidence is identified when this is possible.

3.4.6.4 The analysis of the consequences of the natural external hazards adopted in the design extension envelope shall consider more specifically that these hazards or plausible combinations of hazards are likely to affect:

- several EIPs, particularly redundant or diversified EIPs involved in the same safety function if they are not protected against the hazard or are not robust to it;
- all or part of the installations on a given site, in a lasting manner[18];
- the environment of the installation site (particularly the infrastructures in the vicinity of the installation);
- any off-site provisions to respond to the hazard (mobile equipment resources, fuel supplies, etc.).

III.5 Hazards resulting from malicious acts

3.5.1 The hazards, whether internal or external, resulting from malicious acts shall be taken into account in the design of the installation. The security analysis[19] to be established in application of 5° of I of article R. 1333-4 of the Defence Code with a view to applying for authorisation to hold nuclear materials details the provisions for prevention and for limiting the associated consequences.

3.5.2 Considering the expected effectiveness of the measures planned to protect the installation against malicious acts, the design shall take into consideration:

- the initiating events which, despite the above measures, could result from the malicious acts considered in the security analysis;
- the accident situations that could result from these initiating events.

The consequences of these accidents are assessed in accordance with the provisions of article 3.7 of the order of 7th February 2012 and article 4.7.1 of ASN resolution 2015-DC-532 of 17th November 2015 relative to the safety analysis report of basic nuclear installations.

3.5.3 The measures implemented under article 3.5.1 of this guide and the measures implemented for the demonstration of nuclear safety shall be mutually compatible.

[18] When this is relevant, the design of the measures mentioned in article 3.4.1.2 takes account of the fact that the DEC events, especially the natural external hazards, are likely to affect several installations located on the same site for a long time.

[19] The conditions of performance of this analysis are set in the order of 3rd August 2011 relative to the conditions of performance of the analysis provided for in article R1333-4 of the Defence Code for the protection of nuclear materials and their facilities.

III.6 Utilisation of probabilistic safety assessments

3.6.1 The probabilistic analyses mentioned in article 3.3 of the order of 7th February 2012 and the probabilistic safety assessments (PSA) mentioned in article 8.1.2 of the said order are conducted in order to orient or consolidate the design choices for the systems ensuring a safety function or a support function - particularly in terms of redundancy and diversification - with regard to the objectives mentioned in chapter II.1 of this guide.
The probabilistic analyses and the PSAs shall be used in particular to:

- evaluate the overall frequency of fuel meltdown and the frequency of releases, which contribute to the assessment of the level of safety of the BNI. In practice, the probabilistic safety objective can be broken down into several probabilistic targets which make reference to a restricted perimeter of initiating events or installation operating states. Thus, the guidance values of 10^{-6} per year and per reactor for the frequencies of fuel meltdown caused by initiating events other than hazards for the powered operating states and the shutdown states of the reactor can be adopted;
- shed light on the extremely unlikely nature of the situations mentioned in article 3.2.6;
- highlight any scenarios that make a markedly predominant contribution to the calculated frequency of fuel meltdown or to the calculated release frequencies;
- to assess the robustness of the installation against the hazards, when this is feasible;
- to confirm and if necessary supplement the list of scenarios to consider for the analysis of DEC-A conditions and to verify the adequacy of the measures implemented further to these analyses in order to prevent accidents with fuel meltdown, in relation with the fuel meltdown frequency target expressed in article 2.1.2.3;
- assess the adequacy of the measures chosen to limit the consequences of accidents with fuel meltdown.

3.6.2 The PSAs shall take all the relevant initiating events into account. The PSAs shall more specifically take into account:

- all the initial normal operating states of the installation:
- the events that can affect the reactor and the fuel storage pool simultaneously;
- the events that can affect all the installations on a site simultaneously, including over a long period.

If no proven method exists for certain hazards, or if the necessary data are not available, other methods shall be implemented to assess the safety risk these hazards represent.

The level-1 PSA shall be carried out with a level of detail that is appropriate for the risks. For each initiating event considered it shall establish the accident sequences resulting from the success or failure of the systems and the planned operator actions to ensure the safety functions; it shall allow the identification and evaluation of the frequencies of the sequences leading to fuel meltdown.
The level-2 PSA shall be carried out with a level of detail that is appropriate for the risks. It shall model the physical phenomena that occur during an accident with fuel meltdown and the measures implemented to mitigate the consequences; the level-2 PSA and the supporting analyses shall allow the nature, the extent and the frequencies of releases outside the reactor containment to be assessed.

3.6.3 In accordance with articles 3.3 and 3.8 of the order of 7th February 2012, the probabilistic analyses and the PSAs are carried out in accordance with an appropriate methodology, taking account of available international experience and integrating the technical, organisational and human aspects. The assumptions used in the PSAs shall be as realistic as possible given current knowledge in order to avoid excessive conservatism, which would skew the prioritisation of sequences or the assessment of possible improvements.
The assumptions concerning the conditions of personnel intervention and equipment mission durations shall be appropriate and described in detail.

Article 3.8 of the order of 7th February 2012

I. - The demonstration of nuclear safety is based on:
- up-to-date and referenced data; it takes into account the available information mentioned in article 2.7.2;
- appropriate, clearly explained and validated methods, integrating assumptions and rules adapted to the uncertainties and limits of knowledge of the phenomena in play;
- calculation and modelling tools qualified for the areas in which they are used.

II. - The licensee specifies and justifies its criteria for validating the methods, for qualifying the calculation and modelling tools and for assessing the results of the analyses carried out to demonstrate nuclear safety.

3.6.4 The results of the PSAs shall be presented with analyses of uncertainty and sensitivity, and the limits of the PSA shall be identified insofar as possible.

III.7 Principles for developing analysis methods

3.7.1 In application of article 3.8 of the order of 7th February 2012, the analysis methods used to analyse the events in the design reference envelope and the design extension envelope are described in detail and validated. They are based on qualified calculation tools and approved modelling choices.

3.7.2 When developing an analysis method, the first necessity is to determine the conservative accident scenario(s). The predominant physical phenomena associated with this/these scenario(s) shall then be identified. When the analysis concerns a DBC condition, the parameters influencing these phenomena shall be listed and rendered conservative, but without modifying the physical nature of the scenario.
Furthermore, justified increases in margins shall be applied such that taking into account the physical phenomena that are not explicitly modelled cannot call into question the conclusions of the analyses.

3.7.3 The analysis methods shall detail how uncertainties are taken into account. These uncertainties shall be substantiated, particularly with regard to their method of processing and their combinations, applying conditions that are proportionate to the risks.
Particular attention shall be paid to the parameters that influence the effectiveness of the passive driving forces if they are used.

IV GENERAL RECOMMENDATIONS FOR THE DESIGN

IV.1 Architecture of the safety functions

IV.1.1 General

4.1.1.1 The architecture of the reactor safety functions, that is to say the way in which the safety functions are ensured by the various systems IP for all the situations considered in the design, shall enable the installation to satisfy the objectives mentioned in chapter II.1 of this guide.

4.1.1.2 The specifications of the systems IP resulting from the chosen architecture for the reactor safety functions shall be sufficiently precise to enable each system IP to be designed.

4.1.1.3 In application of the principle of defence in depth set out in II. of article 3.1 of the order of 7th February 2012, the capability of the installation to ensure the safety functions for all the incidents and accidents shall be based on the quality of the specification, design, production and verification of each component, IP on the independence as far as necessary between components IP or systems IP, the redundancy and diversity of the components IP or systems IP as far as necessary, and the consideration of the direct and indirect effects of the incidents or accidents for the design of the structures IP in which the EIPs are installed.

Article 3.1 of the order of 7th February 2012

II. - Application of the principle of defence in depth is based chiefly on:
[…]
- identifying the functions necessary to demonstrate nuclear safety;
- a cautious design approach, integrating design margins and wherever necessary introducing adequate redundancy, diversification and physical separation of the items important for protection that fulfil functions necessary to demonstrate nuclear safety, to obtain a high level of reliability and guarantee the functions mentioned in the preceding paragraph.

4.1.1.4 The use of passive systems, without it being necessary to favour this as a matter of course, can have advantages in certain cases when it is possible to justify the relevance and the effectiveness.

IV.1.2 Independence between EIPs

4.1.2.1 The architecture of the reactor safety functions shall provide sufficient independence between the levels of defence in depth defined in chapter II.2.1 of this guide. This requires sufficient independence between the systems IP involved in different levels of the defence in depth[20].

[20] The similarity of the analysis rules for DBC-2 conditions with those for DBC-3 and 4 conditions is such that the independence between the EIPs considered in the demonstration of nuclear safety associated with these conditions is not required.

4.1.2.2 The independence between systems IP involved in distinct levels of defence is materialised by the independence between their constituent EIPs. The independence between EIPs shall be based on adequate implementation of:

- diversification;
- physical separation or distancing;
- limitation:
    - of shared components, including in the systems ensuring a support function;
    - information that is common or dependent on the same given source;
    - interactions through coupling, synchronisation and communication procedures;

in order to avoid common cause failures and failure propagation between these EIPs.

4.1.2.3 The systems IP fulfilling the safety functions under DBC-2 to 4 and DEC-A conditions shall be as independent as necessary of the systems used during normal operation of the reactor.

4.1.2.4 In order to obtain sufficient independence, the systems IP identified in application of article 3.4.1.2 to manage the DEC-A conditions shall be as diversified as necessary from the systems used in the DBC conditions whose failure they counteract. In this respect, particular attention shall be paid to the design of the systems ensuring a support function.

4.1.2.5 The systems IP fulfilling safety functions during DEC-B conditions shall be, insofar as reasonably practicable[21], independent from the systems used during normal operation of the reactor, and from the systems coming into play in the DBC-2 to 4 conditions or in the DEC-A conditions. In this respect, particular attention shall be paid to the design of the systems ensuring a support function.
The adequacy of the independence is assessed on the basis of deterministic considerations, supplemented where relevant by probabilistic considerations (taking account in particular of the reliability of any shared resources).

IV.1.3 Installation autonomy

4.1.3.1 The installation shall be able to function autonomously for a period compatible with the response possibilities of resources external to the site, particularly with regard to its electrical power supply and the heat sink, to be able to control/manage the events in the design reference envelope and in design extension envelope affecting the reactor or the fuel storage pool, including long-duration events affecting both the reactor and the spent fuel storage pool. A good practice consists in aiming for an autonomy of at least 72 hours.

[21] To give an example, it is considered not to be reasonably practicable for the reactor containment, its penetrations and their isolation components which come into play under DEC-B conditions to be independent of those that come into play under DBC 2 to 4 operating conditions and DEC-A conditions.

IV.1.4 IP systems common to several BNIs or to one reactor and one fuel assembly storage pool:

4.1.4.1 Making EIPs common to several BNIs shall be limited and justified (a natural water reserve or embankment, for example). More specifically, this pooling:

- shall not call into question the shutdown, cooling and residual heat removal from each of the BNIs in the design reference and extension envelopes;
- shall not lead to insufficient autonomy of the electrical power sources and the cooling water necessary for each BNI.

4.1.4.2 The presence of systems IP common to one reactor and to one fuel storage pool:

- shall not call into question the shutdown of the reactor, the cooling and residual heat removal from the reactor and its fuel storage pool in the design reference and extension envelopes;
- shall not lead to insufficient autonomy of the electrical power sources and the cooling water necessary for the reactor and the fuel storage pool.

With this aim in view, the use of independent systems shall take priority.

IV.2 Designing EIPs

IV.2.1 Categorising the safety functions and determining the specified requirements for EIPs

4.2.1.1 The aim of the safety classification for EIPs is to guarantee that they are designed, manufactured and monitored in operation with a quality standard commensurate with their role in nuclear safety.
The classification shall thus take into account the role of the EIPs in:

- preventing and limiting the consequences of the hazards;
- fulfilling the safety functions.

The classification can have several classification levels (several safety classes).

The safety classification shall comprise the following successive steps:

- identification and categorisation of the safety functions established according to their role in nuclear safety;
- identification and classification of the EIPs fulfilling these functions;
- defining appropriate design, manufacturing and in-service monitoring requirements for the EIPs.

4.2.1.2 The safety functions shall be divided into an adequate number of nuclear safety categories established according to their role in nuclear safety, taking into account:

- the consequences of their failure for nuclear safety;
- their estimated frequency of activation;
- the time available for their deployment and the time frames during which the functions shall be ensured, more specifically to achieve a controlled or safe state.

4.2.1.3 The procedure for categorising the safety functions shall be based on a deterministic approach supplemented, when relevant, by probabilistic analyses and expert judgement.

4.2.1.4 The EIP participating in the fulfilment of a safety function shall be classified consistently with the category of that function. The EIP participating in the fulfilment of several safety functions shall be classified consistently with the highest category of these functions.

4.2.1.5 The design of IP systems shall be defined more specifically from the safety functions in which they participate, consistently with the analyses of the DBC/DEC conditions and the hazards. It shall consider in particular:

- the single failure criterion;
- electrical power backup;
- physical separation.

4.2.1.6 The specified requirements applicable to EIPs shall be determined consistently with the design of the systems IP or structures IP to which they belong and with the safety class resulting from the safety functions to which they contribute. This is the case in particular with:

- the use of codified design and construction rules and appropriate standards or technical specifications;
- the in-service monitoring capability, through periodic tests for example;
- resistance to hazards;
- qualification;
- quality assurance.

4.2.1.7 The specified requirements applicable to the systems fulfilling a support function shall be consistent with those of the systems IP served.
When the failure of a support function EIP does not immediately and directly compromise fulfilment of the served function (sufficiently long grace period), this EIP can be assigned to the safety class immediately below that of the served system IP.

4.1.2.8 Within a same given safety class, the EIPs can be grouped into a limited number of families with uniform specified requirements.

4.2.1.9 Any interfaces between EIPs shall be specified and designed to guarantee that the failure of an EIP does not prevent an EIP with a higher requirement level from ensuring its safety functions.

4.2.1.10 When an EIP is called upon to control an event in the design reference envelope - other than a DBC-1 and 2 conditions - or to manage an event in the design extension envelope, its planned duration of operation on this occasion and the conditions to which it is subjected constitute its normal operating condition and - for a nuclear pressure equipment item defined in article R. 557-12-1 of the Environment Code - its normal service situation. The dimensioning of the EIP shall be based on criteria that guarantee compliance with the requisite functional requirements and ultimately its ability to fulfil its function. It is not necessarily based on the same criteria as those used to dimension the systems used in normal operation, but it shall guarantee compliance with the requisite functional requirements.

IV.2.2 Reliability of EIPs and IP systems

4.2.2.1 The EIP and systems IP shall be designed such that the safety functions they fulfil are ensured with due reliability in view of their role for nuclear safety. This reliability is obtained through an appropriate combination of:

- design, production, installation, verification and maintenance measures;
- redundancy, separation and diversification between EIPs in order to reduce the probabilities of common cause failures.

4.2.2.2 The following shall be considered in the design of the EIPs:

- ageing and wear mechanisms (possibly in relation with the maintenance programme);
- uncertainties concerning the physical parameters of the installation;
- operating experience feedback.

4.2.2.3 Insofar as this does not introduce excessive complexity and where a single state fostering nuclear safety is identified, the IP systems shall be designed such that they switch automatically to this state (fail-safe principle) when some of their components have failed (including as a result of failure of a system fulfilling a support function).

IV.2.3 Single failure criterion

4.2.3.1 The systems IP necessary for the control of the design-basis condition categories 2 to 4 (DBC-2 to 4) shall be designed in compliance with the single failure criterion.

4.2.3.2 The active single failure of an EIP shall be postulated when it is called upon, in the short or long term.

4.2.3.3 The passive single failure of an EIP[22] shall be postulated for the long term as from 24 hours after the event necessitating operation of the IP system. The possible leaks in the short term shall be considered for the headers.
Furthermore, it shall be verified through sensitivity analyses that a passive single failure postulated before 24 hours have elapsed or leading to a higher leakage rate than the conventionally defined value (up to the break of a connected pipe of 50 mm inside diameter), would not lead to more severe consequences than those resulting from an active single failure or would not lead to a cliff-edge effect in terms of system IP effectiveness, or in terms of radiological consequences.

[22] The concept of passive single failure does not apply to the main primary system or the main secondary system.

4.2.3.4 Measures to prevent and limit the consequences of passive failures shall be implemented, particularly with regard to detection, isolation and leak collection.

4.2.3.5 Some single failures could be excluded, notably those relative to the opening of certain check valves subjected to high pressure differentials or to the operation of certain equipment items that are not subject to significant load variations, on the basis of appropriate justifications taking into account in particular:

- the design and operating measures implemented;
- an analysis of operating experience feedback;
- if necessary; for active single failures, an analysis of the consequences of the failure conducted with less-conservative rules, methods or assumptions than those adopted for the analysis of the design-basis conditions.

IV.2.4 Qualification of the EIPs

4.2.4.1 In application of II of article 2.5.1 of the order of 7th February 2012, the EIPs undergo qualification with the aim of guaranteeing their capability to meet their specified requirements for the conditions in which they are necessary. These conditions shall include the conditions associated with the environment (such as temperature, pressure, humidity, impact of fluid jets, irradiation, vibration, chemical phenomena, electromagnetic interference and any plausible combination of these factors), and the conditions associated with the transported fluid (such as radioactive fluids, particle-laden water, thermal shock)

Article 2.5.1 of the order of 7th February 2012
II. - The elements important for protection are subject to qualification proportionate to of what they protect, aiming in particular at guaranteeing the ability of these elements to fulfil their assigned functions, with respect to the stresses and environmental conditions associated with the situations in which they are necessary. Design, construction, tests, inspection and maintenance provisions enable this qualification to be maintained for as long as necessary

4.2.4.2 Qualification shall be obtained for the entire planned operating life of the reactor, and even for the final shutdown and decommissioning phases when appropriate. This qualification period may be shorter for components if in-service replacement is possible (in operation or during the final shutdown and decommissioning phase).

4.2.4.3 Qualification shall be based more specifically on analysis, construction, testing, monitoring and maintenance measures.
Qualification methods shall be defined and substantiated. Loadings shall be defined to cover the environmental conditions in accident situations, including situations with core meltdown.
The qualification of EIPs shall take into account ageing and wear mechanisms, and provisions for ensuring and monitoring qualification durability shall be defined during the design phase.

IV.2.5 Taking into account industrial practices, maintenance and in-service monitoring in the design of EIPs, and the constraints relative to their ageing

4.2.5.1 The design shall take into account the constraints inherent to the construction or manufacturing of the installation, and its EIPs in particular, in order to ensure the feasibility and reliability of these operations, including the associated inspection operations, under controlled quality conditions, thereby limiting the risks of deviations between the as-designed installation and the as-built installation.

Taking proven industrial practices into consideration provides the benefit of experience feedback in terms of feasibility, reliability and quality of work performance.

The EIPs whose construction or manufacture requires the finalising of specific techniques or techniques as yet not proven shall be identified during the design phase and given due attention. This can result in the adaptation of specifications (provisions, tolerance ranges, etc.) consistent with the verification capabilities, by mock-ups or prototypes or any other relevant means.

4.2.5.2 The EIPs shall be designed so as to allow their maintenance and in-service monitoring (in-service inspection, periodic tests) in order to verify:

- the integrity of their components and their leak-tightness, particularly when they are designed to contain radioactive fluid;
- the availability and the performance of the system components including, if necessary, when the reactor is in power operation;
- maintaining of the required performance of the systems for all the events in the design reference envelope and the design extension envelope.

4.2.5.3 Measures shall be taken at the design stage to facilitate monitoring of the planned ageing mechanisms and to detect any deterioration or unexpected behaviour that could arise during operation of the BNI.

IV.2.6 Taking decommissioning and site rehabilitation into account in the design phase

4.2.6.1 Final shutdown, decommissioning and the targeted physical state of the installation after decommissioning shall be taken into account at the design stage in order to facilitate performance of the work, with the aim more specifically of:

- enabling decommissioning to be accomplished in as short a time as possible;
- allowing a complete clean-out of the installation, that is to say restoring it to the initial state before activation or contamination of the structures.

The recommendations of the reference guides in this area shall be taken into consideration.

The following shall be kept as low as reasonably practicable:

- radiological exposure of the workers;
- the quantities and chemical and radiological toxicity of liquid and gaseous effluent discharges;

- the quantities and activities of radioactive waste.

In application of article 8 of the decree of 2nd November 2007, the methodological principles and the steps envisaged for installation decommissioning, rehabilitation and subsequent monitoring shall be taken into account at the design stage.

Article 8 of decree 2007-1557 of 2nd November 2007

I.- The application [for authorisation to create a nuclear installation] is accompanied by a file containing: […]

10° The decommissioning plan which presents the methodological principles and the steps envisaged for decommissioning and rehabilitating the installation and subsequent monitoring of the site. The plan provides justification for the dismantling time envisaged between final operational shutdown of the installation and its decommissioning. It can refer to a document drawn up by the licensee for all of its nuclear installations and enclosed with the file .

4.2.6.2 The technical choices at the design stage shall focus more specifically on:

- the design of the equipment items, the layout of the building and the access routes. The equipment items that could contain radioactive substances during normal and incident operation shall be designed so as to facilitate, insofar as possible, their inspection, their radiological characterisation, their post-operational clean-out, their disassembly and their transportation. When appropriate, radiological protection structures which can be easily removed during the decommissioning operations shall be implemented in order to reduce the activation of the materials and equipment. Civil works shall be laid out taking into account the future decommissioning operations, particularly as regards components whose handling is complex. Consideration shall also be given to equipment items that could contain radioactive substances in accident situations;
- the materials: they shall be chosen taking account of their chemical composition and the phenomena to which they are likely to be subjected in order to limit the risks associated with the decommissioning operations and facilitate the subsequent management[23] of the waste produced during these operations.

These technical choices shall be made considering experience feedback from completed or ongoing decommissioning operations or operations to rehabilitate existing sites.

4.2.6.3 The structures, systems and components put in place for normal, incident and accident operation of the installation and whose utilisation is also envisaged in the future installation decommissioning operations, shall be identified. Measures shall be taken to ensure their ability to meet their specified requirements for decommissioning, considering in particular experience feedback from completed or ongoing decommissioning operations or operations to rehabilitate existing sites. These measures shall take into account the planned operating time frame of the reactor, from the duration of the preparatory operations through to decommissioning, and the duration of actual decommissioning operations. Where

[23] Considering the current and foreseeable state of the radioactive waste management routes.

applicable, the replaceability of these structures, systems and components shall be examined at the installation design stage.

4.2.6.4 Provisions enabling the installation site soils to be characterised at the end of its operating life shall be planned for at the design stage.

IV.3 Taking organisational and human aspects into account in the design of the socio-technical system

4.3.1 The installation constitutes a socio-technical system whose functioning is based on the coordination between people, an organisation, technical resources and a physical working environment. The socio-technical system shall be designed so as to create the best possible conditions for the personnel to perform the activities associated with operation of the installation, equally well in normal operation as in incident, accident and hazard situations (design reference and extension envelopes).

The socio-technical system shall thus have a coherent design procedure integrated by all the entities involved in the design of the installation.

The design procedure shall be based on experience feedback and knowledge in the areas of organisational and human factors and operation of the installation, and in particular on nationally and internationally recognised standards[24] and practices.

4.3.2 The design of the socio-technical system shall minimise the possibilities of inappropriate human actions and foster the ability of the personnel to detect and manage unforeseen events, whatever the state of the installation, especially in incident, accident and hazard situations.

4.3.3 The search for design provisions shall be carried out progressively and, if necessary, iteratively, in three phases: analyses leading to the defining of design requirements, the defining of measures and validation of the appropriateness of the envisaged measures for the formulated requirements.

1) The analyses shall serve to specify the design requirements associated with the users' needs and the future organisation. More specifically, the requirements associated with the performance of these users' activities shall be taken into consideration from the start of design. They shall take into consideration the activities the personnel will have to perform and, if they can be determined, the working environment and the organisation of the activities. Appropriate data collection and analysis methods for the activities, complying with the state-of-the-art in this area, shall be used during the design process to identify the requirements relative to human activities. These methods shall be applied and integrated sufficiently early in the design process to provide useful elements for the defining and putting in place of design provisions.

The analyses shall be based in particular on operating experience feedback from nuclear installations in France and abroad, on experience feedback from other industrial sectors, and on studies using simulators, particularly with regard to the control room activities.

Thought shall be given to ensure appropriate division of the tasks between those carried out by the operators and those performed automatically.

The design requirements of the socio-technical system resulting from these analyses shall be formalised and their integration monitored throughout the installation design, construction, commissioning and operation phases.

[24] For example, standard BS-EN-ISO 9241-210 "Ergonomics of human-system interaction. Part 210: Human-centred design for interactive systems", published in January 2011.

2) The design provisions shall render the various components of the socio-technical system effective and efficient in normal operation and in incident, accident or hazard situations alike (design reference and extension envelopes). Particular attention shall thus be paid to:

- the human-machine interfaces (including computerised interfaces), particularly in the control rooms;
- and more generally, wherever humans are required to intervene:
  - to the signalling to identify the premises and the structures, systems and components;
  - to the conditions of access to the premises and the equipment;
  - to the physical working environment (lighting, audio levels, and temperature) in order to ensure conditions fostering correct performance of the activities.

Lastly, the following aspects shall also be taken into consideration:

- the licensee's organisation, particularly in terms of manpower and management of concomitant activities;
- the operational documents intended to guide the personnel in their activities shall be designed such that the personnel can understand the end-purpose and the importance of the activities.

3) The design provisions shall be validated using appropriate assessment methods and means (user tests, mock-ups, simulation, etc.) under conditions that are as representative as possible of those that will be encountered in operation (including the emergency control room). The validation of the operational control means and actions in the main control room shall be carried out using a scale-1 simulator.

4.3.4 The design shall satisfy the general prevention principles set out in article L. 4121-2 of the Labour Code, and its paragraphs 4° and 7° in particular. The choice of processes, the layout of the installation, the work places and the workstations undergo an assessment of the risks for the health and safety of the workers in accordance with article L. 4121-3 of the Labour Code**.**

Article L. 4121-2 of the Labour Code

The employer applies the measures stipulated in article L. 4121-1 on the basis of the following general prevention principles:

…

4° Adapt the work to the worker, particular as regards work station design and the choice of work equipment and work and production methods… ;

…

7° Plan the prevention measures by integrating - into a coherent whole - the technical aspects, work organisation, working conditions, social relations and the influence of ambient factors, …;

Article L. 4121-3 of the Labour Code

The employer, considering the nature of the activities of the enterprise, assesses the risks for worker health and safety, including in the choice of manufacturing processes, work equipment, chemical substances and preparations, arrangement or rearrangement of work places or the installations and the defining of the work stations.

Following this assessment, the employer implements prevention actions and work and production methods guaranteeing a better level of worker health and safety protection…

IV.4 Taking radiation protection into account in the design

4.4.1 The risks associated with the exposure of persons to ionising radiation shall be taken into account as from the installation design phase, in both normal operation and incident or accident situations. With regard to normal operation, particular attention shall be paid to the periods of installation outages for maintenance or fuel reloading. When work in the reactor building is envisaged while the reactor is under power, design measures shall be defined to reduce worker exposure to ionising radiation.

4.4.2 Under the provisions of article L. 593-42 of the Environment Code and articles R. 4451-7 and R. 4451-10 of the Labour Code, and in order to reduce occupational exposure of workers to ionising radiation as much as is reasonably practicable, the progress of technology and practice at the time of design is taken into account, and in particular:

- the materials of the primary cooling system and its auxiliary systems shall be chosen so as to limit the formation of corrosion and activation products;
- design measures shall enable the localised concentrations of radioactive substances in the systems to be limited;
- measures shall enable the frequency and duration of human activities in specially regulated or prohibited zones defined in article R. 4451-20 of the Labour Code to be kept as low as possible, taking into account the layout of the premises, the ease of access to the work locations, the working environment conditions, the development of specific tools and remote operation;
- for application of article L. 4121-2 of the Labour Code, an appropriate layout of the structures, systems and components containing radioactive substances shall, as far as possible, allow a reduction in the duration of work operations, the implementation of effective radiological protections, preferably permanent, and ensure a reasonable distance between the workers and the sources of radiation.

4.4.3 Under the provisions of article L. 593-42 of the Environment Code and articles R. 4451-10, R. 4451-24 and R. 4451-40 of the Labour Code, and in order to avoid any risks of dispersion of radioactive substances, consistently with the provisions of article 3.4 of the order of 7th February 2012:

- appropriate static and dynamic containment measures shall be defined;
- the layout of the premises shall allow movable structures for the containment of radioactive substances to be put in place if necessary for certain operating operations (in-service inspection or maintenance in particular), ;
- radiation protection monitoring and supervision equipment shall be planned for and be:
    - appropriate for the risks at the work stations and in the regular work zones;
    - positioned in locations allowing a representative measure of the radiological conditions and the detection and monitoring of any drift in normal operation and, if necessary, during incident or accident situations, including accidents with fuel meltdown;
    - intended to monitor the level of contamination of workers and their equipment and tools situated in judicious locations in view of the foreseeable movements of personnel and equipment, of sources of contamination and of the activities - especially maintenance - to be carried out;
- measures shall facilitate equipment decontamination and decommissioning operations.

4.4.4 Design provisions shall more specifically allow, in terms of radiation protection, the performance of the human actions planned for in the design reference envelopes and design extension conditions, in accordance with the objectives of article R. 4451-10 of the Labour Code, so as to contribute to their feasibility required under articles 3.3.1.4.5, 3.3.2.3.2, 3.3.3.3.2 and 3.4.4.2.

Article L. 593-42 of the Environment Code

The general rules, prescriptions and measures taken in application of this chapter and of chapters V and VI for the protection of public health, when they concern occupational radiation protection, concern the collective protection measures which are the responsibility of the licensee and designed to ensure compliance with the principles of radiation protection defined in article L. 1333-2 of the Public Health Code. They apply to the design, operation and decommissioning phases and are without prejudice to the obligations incumbent on the employer in application of articles L. 4121-1 et seq. of the Labour Code"

Article R. 4451-7 of the Labour Code

The employer takes the general administrative and technical action, particularly with regard to work organisation and working conditions, necessary for the prevention accidents at work and occupational diseases that may be caused by exposure to ionising radiation…

Article R. 4451-10 of the Labour Code

Individual and collective occupational exposure to ionising radiation are maintained below the limits laid down by the provisions of this Title at the lowest level it can reasonably be expected to achieve.

Article R. 4451-20 of the Labour Code

Inside the controlled area and when the exposure is likely to exceed some of the levels set by a decision from the Autorité de Sûreté Nucléaire taken pursuant to Article R. 4451-28, the employer takes all action to ensure that specially regulated areas are demarcated.

These must have clear signage and are subject to specific access rules.

Article R. 4121-2 of the Labour Code

The employer implements the measures provided in article L. 4121-1 on the basis of the following general prevention principles:

…

8° Take collective protection measures, giving them priority over individual protection measures;

…

Article R. 4451-24 of the Labour Code

In areas where there is a risk of internal exposure, the employer takes all the appropriate measures to avoid any risk of radioactive substances being dispersed inside or outside the area.

Article R. 4451-40 of the Labour Code

The employer defines the collective protection measures appropriate to the nature of exposure which exposed workers are likely to received.

Definition of these measures take into account other potential occupational risk factors in the workplace, in particular when their combined effects are such that they would increase

the effects of exposures to ionising radiation…

V SPECIFIC RECOMMENDATIONS FOR THE DESIGN OF BARRIERS

V.1 Reactor core and associated systems

5.1.1 The design of the reactor core and the associated systems comprises:
- the design of the fuel assemblies;
- the design of the systems for controlling the nuclear chain reactions (absorbing rod cluster control assemblies and associated mechanisms, soluble neutron absorber);
- the design of the equipment items internal to the RPV.

5.1.2 The fuel assembly design shall provide appropriate margins.
More specifically:
- the design of the fuel assemblies shall allow the rapid introduction into the core of mobile absorbing elements (control rod clusters) so as to contribute to the control of the nuclear reactions under the design-basis conditions, in DEC-A conditions (excluding those that postulate failure of control rod insertion) and during design-basis earthquakes;
- the structure of the fuel assembles (guide tubes, grid assemblies, nozzles, etc.) and the fuel cladding shall be designed so as to allow cooling of the fuel in the core under the design-basis conditions, under DEC-A conditions and during design-basis earthquakes.

Furthermore, the fuel assemblies shall be designed to maintain their integrity during storage, transport and handling, before and after irradiation in the reactor.
The fuel design shall prevent losses of leak-tightness in normal and incident operating conditions. The possible presence of a few cladding defects during normal operation shall however be taken into consideration in the safety case and for operations concerning the fuel after its irradiation in the reactor.

5.1.3 The reactor core shall be designed and built such that it withstands the static and dynamic loads to which it is subjected in the design-basis conditions, in DEC-A conditions and during design-basis earthquakes so that the reactor can be shut down safely, maintained in a sub-critical state and cooled.
To this end:
a) the fuel assemblies shall be designed to duly withstand the ambient conditions (chemical, thermal and mechanical effects, irradiation) planned for in the reactor core, and taking account of the risks of damage that can arise under the design-basis conditions, under DEC-A conditions and during design-basis earthquakes. The fuel rod cladding shall provide a barrier that isolates the fuel pellets and the fission products from the primary coolant. By convention, the mechanical analyses also consider the quadratic sum of the effects of reactor coolant pipe breaks postulated in the design reference envelope and the design-basis earthquake;
b) the internal equipment of the reactor pressure vessel shall be designed such that under the design-basis conditions, under DEC-A conditions and during design-basis earthquakes, the following can be carried out:
- cooling of the fuel by the coolant fluid in these situations while maintaining the fuel assemblies in place;
- control of the nuclear reaction by allowing insertion of the mobile absorbing rod clusters.

By convention, the mechanical analyses also consider the quadratic sum of the effects of reactor coolant pipe breaks postulated in the design reference envelope and the design-basis earthquake.

5.1.4 In the event of an earthquake in the design extension envelope, the behaviour of the core (especially the structure of the fuel assemblies), of the RPV internal equipment and of the control rod mechanisms shall not impede shutdown of reactor, maintaining it in sub-critical state and cooling of the fuel.

5.1.5 Monitoring of the confinement of radioactive substances by the fuel rod cladding shall be planned for at the design stage. Monitoring shall be ensured as long as fuel is present in the installation.

V.2 Primary and secondary systems

V.2.1 General recommendations

Article 1 of the order of 10th November 1999

For the application of this order, the following designations are used::

a) Main primary circuit of a nuclear steam supply system: the generating circuit comprising all the pressurised elements of this steam supply circuit, containing the fluid which directly receives the energy given off by the nuclear fuel and which cannot be reliably and securely isolated from that containing this fuel. It comprises the safety accessories and the pressurised accessories playing an isolating role;

b) Main secondary circuit of a nuclear steam supply system (NSSS) : each of the circuits consisting of the the secondary containment of one of the NSSS steam generators and the pipes which cannot be reliably and securely isolated from it, including the safety accessories and the pressurised accessories playing an isolating role;

5.2.1.1 The main primary system and main secondary systems are defined in article 1 of the order of 10th November 1999.

5.2.1.2 Measures shall be taken to guarantee the integrity of the main primary system and main secondary systems equipment during operation of the installation.
These measures shall focus on the following:

- the quality of the design and the associated verification;
- the quality of manufacture and the associated inspections;
- compliance with the conditions for which the equipment items have been designed and manufactured;
- performance of the maintenance and monitoring operations, periodic inspections and the repairs necessary to maintain their level of safety.

These measures aim to prevent the occurrence of equipment failure modes and, if applicable, to detect a damage situation in due time.

V.2.2 Overpressure protection

5.2.2.1 Overpressure protection of the main primary system and the main secondary systems shall be put in place for the various reactor states:

- for the DBC conditions;
- for the DEC-A conditions. The DBC-2 conditions with failure of automatic reactor shutdown are considered in particular;
  The DEC-A conditions that result from the combination of a DBC condition and failure of reactor automatic shutdown shall not lead to a primary pressure that exceeds the reference value corresponding to 1.3 times the design pressure.

This protection complies with the regulatory requirements applicable to directive 2014/68/EU of 15th May 2014[25] relative to pressure equipment (§ 2.10, 2.11 and 7.3 of its appendix I) and of the order of 10th November 1999 (article 4.II.c).

5.2.2.2 For DBC-2 situations as defined in the order of 10th November 1999, the regulation actions, the limitations, the discharge systems and the equipment safety accessories (reactor automatic shutdown - if it meets the essential associated security requirements - triggered by the reactor protection system, pressure relief valves, etc.) can be taken into consideration to demonstrate compliance with the regulatory requirements for overpressure protection if it is demonstrated that they are available in these situations.

5.2.2.3 For the DBC-3 situations as defined in the order of 10th November 1999 and for application of the essential safety requirements 2.10, 2.11 and 7.3 of appendix I to the directive 2014/68/EU of 15th May 2014[26] relative to pressure equipment, automatic reactor shutdown can be considered as a security accessory if it meets the associated essential safety requirements.

5.2.2.2 For the DBC-4 situations as defined in the order of 10th November 1999, the regulation actions, the limitations, the discharge systems and the equipment security accessories (reactor automatic shutdown - if it meets the essential associated security requirements - triggered by the reactor protection system, pressure relief valves, etc.) can be used in the demonstration of nuclear safety if it is demonstrated that they are available in these situations.

V.2.3 "Non-ruptible" components

5.2.3.1 “Break preclusion” shall be implemented for the large components of the main primary system and main secondary systems. This is because no reasonable measure to limit the consequences of their rupture - as an initiating event - could be defined. These components are said to be "non-ruptible".

[25] The essential safety requirements of Appendix I of Directive 2014/68 are rendered applicable to pressure equipment (PE) by article R. 557-9-4 of the Environment Code and to nuclear pressure equipment (NPE) by the order of 30th December 2015 relative to nuclear pressure equipment, which itself is based on article R. 557-12-4 of the Environment Code.

[26] See preceding footnote on the texts that render applicable these requirements of the directive.

This approach shall be underpinned by particularly stringent measures in terms of design, manufacture and in-service monitoring, aiming to prevent rupture. These measures concern:

- the analysis of the relevant damage modes, the choice and utilisation of materials displaying sufficient resistance to these damage modes, the determining of the loads to which they are subjected, including if a hazard occurs, and verification of compliance with the criteria serving to prevent the risks of rupture;
- the use of manufacturing and inspection processes that can demonstrate achievement of a very high standard of quality taking into account, in accordance with point 4 of the preliminary observations of annex I to directive 2014/68 of 15th May 2014 relative[27] to pressure equipment, the "*state of the art and current practice at the time of design and manufacture, as well as of technical and economic considerations which are consistent with a high degree of protection of health and safety protection*";
- in-service monitoring, allowing, for example, the absence of component damage to be verified in good time.

In view of this, the conservative determination of the loads applied, the analysis of the behaviour of the structures under these loads, the existence of margins with respect to the mechanical criteria in particular, the qualification of the manufacturing and procurement processes, the choice, extent and precision of the inspection techniques with respect to the manufacturing processes, the determining of acceptance criteria for manufacturing defects, the in-service accessibility of the areas to monitor and the extent of the associated checks, the integration of experience in the behaviour of similar materials or installations, are means necessary for the implementation of this procedure.

V.2.4 Other considerations associated with the main primary system

5.2.4.1 In application of the principle of defence in depth mentioned in chapter II.2.1, breaks in the primary system pipes shall be considered as SIEs in the demonstration of nuclear safety and measures shall be taken to limit the consequences of such breaks.
The loadings resulting from these breaks are to be taken into consideration for the dimensioning of the fuel assemblies in particular, and for the dimensioning of the internal structures of the primary components (reactor pressure vessel, steam generators, reactor coolant pumps) and of the reactor containment and its internal structures.

By convention, the mechanical analyses of the main primary system consider the quadratic sum of the effects of the reactor coolant pipe breaks postulated in the design reference envelope and the design-basis earthquake;

5.2.4.2 The principle of the "break preclusion" for piping consists in not addressing the consequences of the piping break because the break can be considered extremely unlikely with a high degree of confidence. This “break preclusion” can only be considered for the main reactor coolant pipes and necessitates elements:

- demonstrating that the design, manufacturing and in-service monitoring provisions are such that break can be considered extremely unlikely with a high degree of confidence. In this respect, the recommendations of article 5.2.3.1 apply to these measures;

[27] See above footnote on the texts that render applicable these requirements of the directive.

- demonstrating that this choice is reasonable considering the advantages and drawbacks it brings to the overall level of safety of the installation and to radiation protection.

If "break preclusion" is adopted, only the break (up to a double-ended guillotine break) of the branch pipes connected to the main reactor coolant pipes are to be taken into consideration as SIEs in the demonstration of nuclear safety.
The resulting loadings are to be taken into consideration for the dimensioning of the fuel assemblies, of the internal structures of the primary components (reactor pressure vessel, steam generators, reactor coolant pumps) and of the reactor containment internal structures.
Furthermore, by convention:

- the double-ended guillotine break of the main reactor coolant pipe is considered for the design of the safety injection system, of the reactor containment and the associated systems, and for the qualification profiles of the equipment present in the reactor containment, using appropriate assumptions;
- the double-ended break of the main reactor coolant pipe is considered for determining the loads for the design of the large component supporting structures.

As the use of this assumption is a determining choice, its use and its conditions of application will have to be examined at an early stage of the design. This examination will also address the conditions of implementation.

5.2.4.3 The layout of the primary system pipes shall be such that the postulated failure of a loop of the primary system, including the maximum possible break, does not lead to the failure of another loop. The layout of the primary system pipes and the secondary system pipes shall be such that the postulated failure of a primary system pipe does not lead to the failure of a main secondary system pipe.

5.2.4.4 For the operating phases in which the main primary system is closed, appropriate instrumentation shall be provided to monitor the radiological activity of the primary coolant and any leaks from the main primary system. Design provisions shall allow a periodic assessment of main primary system leakage during operation of the reactor.

5.2.4.5 The occurrence of an SIE taken into consideration under the category-2 design-basis conditions (DBC-2) should not induce release of primary coolant into the containment. This can be verified using all the available equipment. In this case the availability of the equipment in the situation in question shall be demonstrated.

5.2.4.6 The operation of the system protecting the main primary system against overpressure situations shall not lead to the release of radioactive substances directly into the environment.

5.2.4.7 In the cold shutdown states, protection of the main primary system and of the system cooling the reactor in these states shall be put in place to prevent risks of cold overpressure.

5.2.4.8 In order to prevent containment bypasses, the devices ensuring overpressure protection of the systems connected to the main primary system and carrying coolant fluid shall be situated inside the reactor containment or, failing this, in a room with suitable ventilation and appropriate treatment of its atmosphere (filtration for example).

V.2.5 Other considerations associated with the main secondary systems

5.2.5.1 In application of the principle of defence in depth mentioned in chapter II.2.1, breaks in the main secondary systems pipes shall be considered as SIEs in the demonstration of nuclear safety and measures shall be taken to limit the consequences of such breaks.
The loadings resulting from these breaks are to be taken into consideration for the dimensioning of the internal structures of the steam generators and of the reactor containment and its internal structures.

By convention, the mechanical analyses of the main secondary systems consider the quadratic sum of the effects of the pipe breaks postulated in the design reference envelope and the design-basis earthquake;

5.2.5.2 The "break preclusion" can only be considered for the main steam pipes and necessitates elements:

- demonstrating that the design, manufacturing and in-service monitoring provisions are such that break can be considered extremely unlikely with a high degree of confidence. In this respect, the recommendations of article 5.2.3.1 apply to these measures;
- demonstrating that the significant hydrodynamic effects are avoided and that the fixed points are as close as possible to the reactor containment penetrations;
- demonstrating that this choice is reasonable considering the advantages and drawbacks it brings to the overall level of safety of the installation and to radiation protection.

If this assumption is adopted, by convention the masses and energies released by the double-ended guillotine break of the main steam pipe are considered for the design of the reactor containment and the associated systems, and for the qualification profiles of the equipment present in the reactor containment, using appropriate assumptions;

As the use of this assumption is a determining choice, its use and its conditions of application will have to be examined at an early stage of the design. This examination will also address the conditions of implementation.

5.2.5.3 The possibilities of common cause failures of the main steam pipe and of the main feedwater pipes shall be reduced as much as possible by adequate separation of the systems. Whatever the case, the break of any pipe connected to main secondary system pipes which could become separated from its branch connection shall be considered in the demonstration of nuclear safety.

5.2.5.4 The layout of the main secondary system pipes shall be such that the postulated failure of one of them does not lead to the failure of another pipe in the main secondary systems, with the exception of the small-diameter pipes as defined in article 3 of the order of 10th November 1999.

The layout of the primary system and secondary system pipes shall be such that the postulated failure of a pipe in a secondary system does not lead to failure of a pipe in the main primary system, with the exception of the small-diameter pipes as defined in article 3 of the order of 10th November 1999.

5.2.5.5 For the operating phases in which the removal of heat from the primary coolant is ensured by the steam generators, instrumentation shall be provided to continuously monitor each steam generator for any primary system leak.

V.3 3rd barrier

V.3.1 General recommendations

5.3.1.1 To meet the safety objectives mentioned in chapter II.1 of this guide, the 3rd barrier shall be designed so as to limit releases during the short- and long-term phases of the accidents considered in the demonstration of nuclear safety.

5.3.1.2 To this end, the requirements relative to the mechanical strength and the leak-tightness of the 3rd containment barrier shall be set for the design reference envelope and the design extension envelope. The 3rd barrier shall be designed and constructed to meet these requirements.

5.3.1.3 More specifically, the reactor containment, the containment penetrations and their isolation systems shall be designed such that they ensure effective confinement of radioactive substances:

- without necessitating an active system for removing the residual power from the reactor containment for several hours after a core meltdown accident, so as to guarantee a sufficiently long period of grace to deploy an active systems which can fulfil the safety functions under the prevailing conditions;
- in the event of an overall deflagration of the maximum quantity of hydrogen that could be contained in the reactor containment during an accident with core meltdown or after fast local deflagration, taking into account the measures intended to reduce the hydrogen concentration in the containment;
- taking into account the other combustible gases that can be produced in a core meltdown situation, particularly during corium-concrete interaction.

To this end and to whatever extent necessary:

- devices such as hydrogen ignitors or recombiners shall be installed to limit the hydrogen concentration in the containment;
- specific provisions (for example the geometry of the internal compartments of the reactor building or reinforced compartment walls) shall be implemented to prevent phenomena such as fast local hydrogen deflagrations or hydrogen deflagration-detonation transitions or to limit their consequences.

V.3.2 Penetrations and openings in the reactor containment

5.3.2.1 The reactor containment shall feature as few penetrations and openings as possible.

5.3.2.2 The outer part of reactor containment penetrations and openings shall, unless specifically justified, be located into peripheral buildings with adequate containment capacities.

5.3.2.3 Qualification and leak-tightness requirements shall be defined for the containment penetrations in normal operation and in incident and accident situations, in relation with the safety objectives mentioned in chapter II.1 of this guide. Provisions shall be defined for the verification of compliance with these requirements over the lifetime of the installation.

5.3.2.4 The reactor containment penetrations shall feature component(s) allowing them, when necessary, to be reliably sealed in the design reference envelope and the design extension envelope; closing shall be ensured within times that allow the objectives mentioned chapter II.1 of this guide to be achieved.

The penetrations situated on systems connected to the main primary system which could carry primary coolant in incident or accident situations, or connected to systems that communicate directly with the reactor containment atmosphere, shall - unless specifically justified - be equipped with at least two isolation components mounted in series.

Whatever the penetration, one isolation component shall be situated outside the reactor containment (the other being inside the containment if there are two components). The isolation components shall be situated as close to the reactor containment as possible.

5.3.2.5 When in a normal reactor outage state, if the access hatch to the reactor containment equipment is open and fuel assemblies are present in the RPV, it shall be possible to close the access hatch rapidly in the event of an incident or accident leading to radioactive releases in the reactor containment and, whatever the case, within a time frame that allows the objectives mentioned in chapter II.1 of this guide to be achieved.

5.3.2.6 Personnel access airlocks inside the reactor containment shall be equipped with doors with interdependent locking systems so that at least one of the doors is closed when necessary.

5.3.2.7 The consequences of a break in a system which transports radioactive fluid outside the reactor containment during normal operation shall be taken into account, and more specifically:

- the design of the premises housing this system shall take into account the possible effects of this break (overpressures, creation of explosive atmospheres, difficulty in gaining access to the premises, etc.) ;
- a ventilation system and appropriate treatment of the atmosphere (by filtration for example) shall be put in place for these premises when necessary.

5.3.2.8 The possibilities of leakage in the systems transporting radioactive fluid outside the reactor containment in the design reference envelope or under design extension conditions shall be taken into consideration. More specifically, if such systems are used for the management of incidents and accidents, including accidents with core meltdown, these leaks shall be taken into consideration in the assessment of the radiological consequences.

VI RECOMMENDATIONS SPECIFIC TO CERTAIN SAFETY FUNCTIONS

VI.1 Control of nuclear chain reactions in the core

6.1.1 The means for controlling core reactivity shall:
- ensure rapid automatic shutdown of the reactor;
- ensure the achievement of sub-criticality corresponding to the targeted safe state level;
- overcome a failure of reactor automatic shutdown;
- guarantee the absence of criticality in the states in which the RPV is open;
- prevent unintentional attaining of critical conditions in states where the RPV is closed and the reactor is shut down in normal operation.

6.1.2 Reactor shutdown shall be ensured by two independent and diversified means, with at least one of these means being capable of rapidly rendering the reactor sub-critical[28]. These means aim jointly at ensuring core sub-criticality until the reactor reaches a controlled state, then maintaining sub-criticality with an adequate margin to achieve the safe state.
A possible return to criticality can only be accepted in certain rare situations. In this case it shall be of short duration and lead to low nuclear power. It requires specific justification.

6.1.3 When the core is critical, the neutronic design of the core shall ensure intrinsically stable behaviour through the effect of neutron feedback, whatever the power level.
In this respect:
- the void coefficient of reactivity of the primary coolant shall be negative by design;
- the moderator temperature coefficient shall be negative from the zero power hot conditions through to normal operating conditions, with all rod cluster control assemblies (RCCA) at the top of the core. Nevertheless, subject to appropriate justification, a few RCCAs may be inserted temporarily into the core to guarantee the negative moderator temperature coefficient at low power at the beginning of the cycle.

The neutron design of the core shall be such that the void effect is always negative in incident or accident situations.

6.1.4 In the event of abnormal changes in the physical parameters associated with the reactivity, automatic devices shall ensure reactor shutdown with a very high level of reliability.
The duration of complete insertion of the RCCAs and of reactor shutdown shall be justified for the conditions necessitating automatic reactor shutdown.

6.1.5 Ensuring a very high level of reliability of the automatic reactor shutdown function shall be based in particular on the diversification of its main components (physical measurements, signals and associated processing, reactor automatic shutdown circuit breakers).

6.1.6 Design measures shall be planned for to control the specific risks associated with an abnormal reduction in the concentration of soluble neutron absorber.

6.1.7 Systems shall permanently monitor the soluble neutron absorber concentration in the primary system water and the nuclear reactions, from the moment one fuel assembly is present in the RPV. These

[28] Apart from DEC-A conditions which postulate its unavailability.

systems shall more specifically allow the implementation of automatic or manual actions to prevent criticality being reached during incidents or accidents initiated in the reactor outage states in normal operation.

6.1.8 When the core is fully loaded, redundant neutron instrumentation and redundant thermohydraulic instrumentation distributed inside and outside the core shall allow:

- continuous monitoring of the nuclear chain reactions;
- monitoring and prevention, during power operation, of the risks of damaging the fuel, by using in particular a system delivering sufficiently precise information on the distribution of power within the core.

Furthermore, neutron instrumentation shall allow three-dimensional mapping of the neutron flow distribution in the core to be established when the core is critical. Particular justification is required if the first neutron flow map can only be produced from a non-negligible power level. The power level shall nevertheless remain as low as reasonably practicable.

VI.2 Removal of the thermal heat produced by the radioactive substances and nuclear reactions

VI.2.1 Systems for removing residual power from the core

6.2.1.1 Systems shall remove the residual heat from the core after reactor shutdown under DBC and DEC-A conditions; they shall enable the reactor to be brought to and maintained in a safe state.

VI.2.2 System(s) for the safety injection of water into the core

6.2.2.1 Design provisions shall be planned for to cope with the specific risks associated with an accidental reduction in the quantity of water present in the main primary system.
One or more systems shall enable the primary system water inventory to be restored to and maintained at a sufficient level for the design-basis conditions and the DEC-A conditions that require this. The system(s) participate(s) in the removal of residual power from the core.

6.2.2.2 If the design of this/these system(s) provides for reuse of the primary system water that is present in the reactor containment, the phenomenon of water intake clogging and the effects that the debris can have downstream of the water intake - including on the fuel in the core - shall be taken into consideration in the design.

VI.2.3 Primary system depressurisation in accident situations

6.2.3.1 To ensure adequate protection against core meltdown in the event of failure of the systems removing power from the primary system, a means of depressurising the primary system shall be provided to allow the injection of sufficient quantities of water to remove the residual heat produced in the core.

6.2.3.2 A depressurisation system that is as independent as far as reasonably practicable of the system mentioned in article 6.2.3.1, shall help render situations of core meltdown with high pressure maintained in the primary system extremely unlikely with a high degree of confidence. The system shall also fulfil its functions in the event of total long-duration loss of the on-site and off-site alternating current (AC) electrical power sources.

VI.2.4 Removal of heat from the reactor containment

6.2.4.1 In order to preserve the integrity of the reactor containment, systems shall be provided to remove the residual heat from the containment without voluntary release of radioactive substances, under the design-basis conditions and under DEC-A and DEC-B conditions.

6.2.4.2 Removal of residual heat from the reactor containment during an accident with core meltdown shall be based on a system which is as independent as far as reasonably practicable of the systems used to evacuate the residual heat in the design-basis conditions and DEC-A conditions.
If the implementation of this system necessitates an electrical power supply, this power supply shall be backed up by a source which is dedicated as far as reasonably practicable to the mitigation of the consequences of accidents with core meltdown.
In addition:

- if the utilisation of this system leads to the circulation of radioactive fluid circulate outside the reactor containment, the possibilities of this system leaking shall be taken into consideration at the design stage. They shall not call into question the ability of the system to fulfil its mission with regard to the safety objectives mentioned in chapter II.1 of this guide;
- if the design of this system provides for reuse of the water that is present in the reactor containment, the phenomenon of water intake clogging and the effects that the debris can have downstream of the water intake shall be taken into consideration in the design.

VI.3 Containment of radioactive substances;

VI.3.1 Design of the EIPs ensuring radioactive substance containment

6.3.1.1 In application of III of article 3.4 of the order of 7th February 2012, the containment of radioactive substances is ensured by static systems, supplemented if necessary by dynamic systems.

6.3.1.2 The structures IP and systems IP ensuring the containment of radioactive substances shall be designed and built so as to ensure the effectiveness of this function equally well in normal operation as in incident and accident situations, in order more specifically to:

- avoid direct leaks of radioactive substances into the environment from the reactor containment and the situations that can lead to bypassing of the reactor containment;
- ensure effective containment in normal operation and during incidents and accidents, including an accident with core meltdown.

Article 3.4 of the order of 7th February 2012
III. - The function of radioactive substance containment is ensured by placing one or more successive and sufficiently independent barriers between these substances and people and the environment, and if necessary by a dynamic containment system. The number and effectiveness of these systems are proportional to the potential extent and impact of the radioactive releases, including in the event of an incident or accident.

6.3.1.3 The containment shall display the best possible effectiveness in order to achieve the safety objectives mentioned in chapter II.1 of this guide. In this respect:

- leak-tightness criteria shall be defined for the reactor containment and its penetrations;
- leak-tightness criteria shall also be defined for the other buildings of the nuclear island in which radioactive substances are or could be present;
- the dynamic containment systems shall be equipped with a suitably effective filtration system.

6.3.1.4 Means shall be provided for detecting possible leaks of radioactive fluid in the peripheral buildings and the reactor containment and for limiting their consequences.

6.3.1.5 The design shall provide for the use of redundant and, if necessary, diversified means of isolating the systems connected to the main primary system, and provide for the possible failures of these means and detection equipment associated with these failures.

6.3.1.6 Design measures shall be implemented to stabilise the corium inside or outside the RPV, to avoid reactor containment basemat melt-through by the molten core and to ensure the resistance of the reactor containment and the associated devices against any hydrogen deflagration.

VI.3.2 Containment in normal operation

6.3.2.1 Systems shall be provided to control the pressure and temperature in the reactor containment during normal operation and to detect, monitor and, when necessary, treat the radioactive substances that could be released into the atmosphere from the reactor containment.

VI.3.3 Containment of buildings

6.3.3.1 Buildings accommodating systems and components which contain or could contain radioactive substances in normal operation and in incident and accident situations, particularly buildings with penetrations entering the reactor containment and buildings housing systems and components transporting radioactive fluids which could, in case of failure, lead to releases, shall guarantee appropriate

static sealing. If necessary, systems shall be put in place to collect and treat these substances before they are discharged into the environment in gaseous or liquid form.
The number of reactor containment penetrations shall be kept as low as possible to limit the risks of containment bypassing.

VI.3.4 Ventilation systems

6.3.4.1 The ventilation systems shall be designed such that they:

- reinforce as much as necessary the static containment systems by creating a cascade of negative differential pressures leading from the premises with low contamination risk towards the premises or equipment displaying a higher risk in order to prevent the dispersion of radioactive substances in the installation (internal containment) and to direct the gaseous effluents towards appropriate treatment systems (filter, iodine trap) before they are discharged into the environment;
- maintain acceptable ambient conditions for workers during normal operation and in incident and accident situations (temperature in the premises, hydrogen and nitrogen contents, radiation protection and accessibility to the premises during incidents and accidents);
- avoid the creation of explosive atmospheres (air renewal rate) ;
- limit the risks of release of radioactive substances into the environment in case of fire;
- maintain, in normal operation and in incident and accident situations, ambient conditions that are compatible with the operation and the qualification conditions of the EIPs ensuring a safety function.

VI.3.5 Monitoring and periodic tests

6.3.5.1 The reactor containment, the containment penetrations and their isolation systems, shall be designed and built such that tests can be performed to verify compliance with the criteria mentioned in article 6.3.1.3 prior to reactor commissioning, then periodically during the inspections mentioned in article 8.1.1 of the order of 7th February 2012.

Article 8.1.1 of the order of 7th February 2012

The effectiveness of the reactor containment is verified in particular:

- before commissioning, by an initial acceptance test;
- after commissioning and until final shutdown, by periodic tests scheduled so that results figuring in the review report provided for in article L. 593-19 of the environment code date back less than thirty months;
- after final shutdown, under conditions set by the authorisation decree or the prescriptions issued by ASN for its application.

Design measures shall be taken so that the actual containment effectiveness of the reactor containment during normal operation can be determined with sufficient reliability and can be assessed during incidents and accidents, including with core meltdown.

6.3.5.2 To verify compliance with the criteria mentioned in article 6.3.1.3, the nuclear buildings housing systems and components containing radioactive substances shall be designed and built such that it is possible:

- to perform tests to demonstrate the effectiveness of containment of radioactive substances before commissioning the BNI, then periodically thereafter throughout its lifetime;
- or to prove their performance through analysis, in view of the construction and operating measures adopted.

6.3.5.3 Design measures shall allow monitoring of the performance of the dynamic containment and effluent filtration/purification systems prior to discharge into the environment.

VII OTHER SPECIFIC DESIGN RECOMMENDATIONS

In this chapter VII, the use of the term "system" does not prejudge the classification of this system as an EIP or not.

VII.1 Design of systems fulfilling a support function

VII.1.1 Design of the systems removing heat to and from the heat sink

7.1.1.1 The architecture, the specified requirements and the reliability of the systems removing the heat produced by the fuel and dissipated by the various systems, structures and components towards the heat sink shall be consistent with the architecture and the overall requirements defined for the EIPs that cool them.

7.1.1.2 Measures shall be taken to prevent risks of heat sink failure associated with external hazards. The need for specific measures, such as the distancing or diversification of water intakes, or the constitution of an emergency reserve shall be assessed on the basis of a characterisation study of the site and an assessment of the vulnerability of the main heat sink.

7.1.1.3 In order to place several barriers between the systems carrying radioactive fluid - especially the primary coolant - and the environment, the design of the systems carrying heat to the heat sink shall include an intermediate cooling system between the heat exchangers cooling the systems carrying the radioactive fluid and the systems carrying the raw water.

VII.1.2 Electrical power supply

VII.1.2.1 General recommendations

7.1.2.1.1 The electrical power supply for the installation shall comprise a normal power supply system and an emergency power supply system.

7.1.2.1.2 The risks of common cause failure of the electrical components, particularly the electrical panels, shall be reduced, if necessary through appropriate diversification.

VII.1.2.2 Normal electrical power supply system

7.1.2.2.1 To reduce the risks of loss of the off-site electrical power supplies, the normal electrical power supply system shall be connected to the national electricity grid by at least two electric lines. These two lines shall be sufficiently independent of each other.

7.1.2.2.2 The architecture and the devices for protecting or isolating the electrical power distribution system within the installation shall be such that operation of the normal electrical power supply outside the specified variation ranges does not prejudice the availability of the components of the emergency electrical power supply system and the supplied EIPs.

VII.1.2.3 Emergency electrical power supply system

7.1.2.3.1 The emergency electrical power supply system includes the circuits and components necessary for the production, conversion and distribution of electrical power to the electricity-dependent systems fulfilling a safety function.

7.1.2.3.2 The emergency electrical power supply system shall be capable of delivering electrical power to the systems necessary for the fulfilment of the safety functions assuming loss of the normal electrical power supply system in accordance with the functional requirements (power, mission duration, etc.) of the supplied EIPs.

7.1.2.3.3 The emergency electrical power supply system can be supplied by the normal electrical power supply system (off-site sources) and it shall, whatever the case, include dedicated internal emergency sources such as batteries and electrical power generators (diesel generator sets, turbine generator sets, etc.) or any other stand-alone electrical power source.

7.1.2.3.4 The architecture, the defined requirements and the reliability of the emergency electrical power supply system shall be consistent with the architecture and all the specified requirements of the systems ensuring a safety function that are energized by this power supply.

7.1.2.3.5 The principle of independence set out in chapter IV.1.2 of this guide shall be applied to the redundant channels of the emergency electrical power supply system. This independence shall not be compromised by the interconnections to the normal electrical power supply.

7.1.2.3.6 The systems and components which, despite not being EIPs, would nevertheless be supplied by the emergency electrical power supply system, shall not compromise its functional independence, its performance or its reliability in fulfilling the safety functions.

7.1.2.3.7 The electrical power supplies of the instrumentation and control systems that come into play during events in the design reference envelope or the design extension envelope shall satisfy the functional requirements of the instrumentation and control systems they supply. These shall be uninterruptible power supplies.

7.1.2.3.8 The autonomy of the batteries necessary to provide electrical power to the EIPs that fulfil safety functions shall satisfy the functional requirements of the supplied EIPs. Where applicable, it takes into account realistic times[29] for recovery of the normal and emergency power supply systems, particularly in the case of an event in design extension envelope.

[29] "Realistic" in this context means taking experience feedback and degraded conditions into account.

VII.1.3 Thermal conditioning systems

7.1.3.1 Thermal conditioning systems (ventilation, heating, air conditioning) shall guarantee that the ambient conditions in the premises do not affect the functioning of the EIP situated in them.
The architecture and the specified requirements of the thermal conditioning systems shall be consistent with the architecture and the specified requirements of the systems they support.

VII.2 Volumetric and chemical control of the primary coolant

7.2.1 In normal operation, one or more systems shall allow the physical-chemical characteristics of the primary coolant to be controlled, in order more specifically to:

- limit corrosion of the primary system and the fuel cladding;
- maintain the radioactivity in the primary system and the systems connected to it at a level that is as low as reasonably practicable, particularly by the purification of radioactive substances (including the activated corrosion products and the fission products from the fuel) in the primary coolant.

If the system(s) carries (carry) hydrogen, it (they) shall be designed so as to minimise the risk of hydrogen explosion.

7.2.2 During normal operation, a system shall allow adjustment of the quantity of water in the main primary system and of its concentration of soluble neutron absorbent.

VII.3 Nuclear fuel handling and storage

VII.3.1 Handling fuel assemblies

7.3.1.1 The fuel handling systems shall be designed to:

- allow the precise identification of each fuel assembly inserted into or removed from the RPV;
- allow fuel inspections;
- prevent any damage to the fuel assembly structure or cladding during handling, including in incident and accident situations (earthquake, loss of electrical power supplies);
- prevent any falling of fuel assemblies during handling, including in incident and accident situations (earthquake, loss of electrical power supplies);
- prevent any heavy objects from falling onto the fuel assemblies - objects such as transport packages, travelling cranes - or other objects that could damage them, including in incident and accident situations (earthquake, loss of electrical power supplies);
- allow a fuel assembly to be put down in a safe position during handling when this is necessary, including in incident and accident situations (earthquake, loss of electrical power supplies).

7.3.1.2 The buildings in which fuel assembly handling operations take place shall have suitable containment in order to achieve the safety objectives mentioned in chapter II.1 of this guide.

VII.3.2 Dry storage of fresh fuel assemblies

7.3.2.1 The design of the dry storage of fresh fuel assemblies shall enable the safety functions to be fulfilled, including in case of hazards.

7.3.2.2 The design of the dry storage of fresh fuel assemblies shall guarantee the absence of any situation of criticality with specified margins by physical means or processes, under normal storage conditions and during incidents and accidents (particularly for hazards) which could alter the conditions of moderation given the presence of water.

VII.3.3 Underwater storage of fuel

7.3.3.1 The underwater storage of fuel assemblies shall be designed such that its capacity is sufficient to accommodate at any moment the entire content of the core loaded into the reactor pressure vessel.
The storage capacity of the fuel assemblies in the facility shall be determined more specifically according to:

- the power of the reactor;
- the envisaged fuel management methods;
- the projected time frame of operation of the reactor and the spent fuel storage or treatment routes (existing or planned).

7.3.3.2 The fuel assembly storage facility shall be designed such that it guarantees the absence of any situation of criticality, with specified margins, under normal storage conditions and during incidents and accidents.

7.3.3.3 Under article 3.2.6, the fuel storage facility shall be designed such that non-uncovering of the spent fuel assemblies can be guaranteed during storage and handling.

7.3.3.4 The fuel storage facility shall be designed so as to guarantee a level of irradiation in the building compatible with the planned activities of workers and other necessary personnel under normal storage conditions and in incident and accident situations.

7.3.3.5 The fuel storage pool shall be provided with a main cooling system which in normal operation removes the residual heat and maintains the operating conditions of the pool water treatment and purification systems and the systems involved in the containment of the building housing the pool.

7.3.3.6 In the design-basis conditions, or during a design-basis hazard or DEC-A conditions involving loss of the main cooling system of the fuel pool only (used in DBC conditions), the design of the installation shall allow the pool water to be maintained at a temperature below boiling temperature with a sufficient margin in view of the estimated frequency of the event in question.

7.3.3.7 In the event of total loss of the pool water cooling systems, one system or more shall:

- prevent uncovering of the fuel assemblies by compensating sufficiently for the loss of water by boiling;
- establish a level of water in the pool that is sufficient to put the cooling system back into service.

7.3.3.8 It shall be possible to start and operate of a cooling system for the fuel storage pool after prolonged loss of cooling having led to boiling, and to achieve and maintain a safe state.

7.3.3.9 Permanent monitoring of the fuel storage pool water level and temperature shall be provided for. The fuel storage pool shall have means of checking the chemical composition and radioactivity of the cooling water. The fuel storage pools shall have means of detecting and collecting leaks where necessary.

7.3.3.10 By design it shall be impossible for a leak or break in a system connected to the fuel storage pool to lead to exposure of the fuel assemblies in storage or during handling.

Whatever the case, the bottom section(s) housing the fuel assembly storage racks shall not have any connected lines, shall not be able to be emptied by siphoning and shall not be uncovered due to loss of water affecting an adjacent compartment.

7.3.3.11 The dimensioning of the storage compartment structural elements shall include substantial margins with respect to the potential loadings (design-basis earthquake, dropped load, thermal stresses due to boiling, etc.).
The structural elements shall be sufficiently resistant for the fuel storage compartment to fulfil its safety functions in the event of an earthquake in the design extension envelope.

VII.3.4 Actions on the fuel assemblies during operation

7.3.4.1 Design provisions shall exclude any situation of criticality resulting from damage to one or more fuel assemblies during their transportation, handling, storage in the facility or during repair or examination operations.

VII.4 Instrumentation and control

VII.4.1 Instrumentation and control design rules

7.4.1.1 The instrumentation and control architecture shall be designed:

- such that the instrumentation and control (I&C) functions meet the requirements associated with their safety classification;
- with a view to ensuring sufficient independence between the functions associated with different levels of defence in depth;
- taking the plausible failures into account. More specifically, the consequences of spurious activation of equipment due to failure of a component in the I&C systems shall be considered in order to identify any weak spots in the separation of the redundant equipment and in the I&C systems, and to improve the design wherever necessary.

7.4.1.2 A functional analysis shall enable the actuators to be optimally distributed among the various equipment items in order to prevent the occurrence of a DBC-3 or 4 condition, or the loss of a safety function further to the failure of a single physical component.

7.4.1.3 The I&C design, and the digital systems in particular, shall obey predetermined rules designed to prevent the introduction of faults into a system. These rules shall be applied throughout the system life cycle, including its specification, production, operation and maintenance.

7.4.1.4 Fault avoidance shall be supplemented by an analytical approach aiming to eliminate the faults. This approach shall include procedures such as inspections, proof-reading, audits, reviews, accuracy tests, static analyses and various validation tests with analysis of test coverage.
The depth of the analyses and justifications is commensurate with the level of requirements incumbent on the I&C system.

7.4.1.5 The design shall incorporate measures to limit the consequences of any faults that might subsist despite the measures taken to avoid and eliminate them. Thus, as part of the defence in depth, it is necessary in particular to:

- put in place functional diversification of the automatic reactor shutdown functions in order to compensate for a hypothetical error in the specification or the performance of certain functions, by using other functions targeting the same objectives on the basis of different physical signals;
- compensate, by a diversified means, for a hypothetical common cause technical failure of the protection system in certain situations identified in particular by the installation probabilistic safety assessments;

- take into consideration the possibilities of failure of the systems ensuring the instrumentation and control of the functions required to achieve a safe state.

A balance shall be obtained between the effectiveness resulting from the diversification and the complexity it introduces.

VII.4.2 Instrumentation

7.4.2.1 Instrumentation shall be provided to measure the main quantities characterising the nuclear reactions, the tightness of the fuel cladding, the effectiveness of fuel cooling and the state of containment of the nuclear island buildings, and to obtain the information on the installation that is necessary in order to operate it reliably and safely while limiting adverse effects for the interests mentioned in article L. 593-1 of the Environment Code. The instrumentation shall be appropriate (measurement range, location, qualification, uncertainty, etc.) for the situations in which it is required.

7.4.2.2 The instrumentation and the methods of automatic recording of the relevant quantities for assessing nuclear safety shall be chosen and designed in order to have the necessary information and to detect an incident or accident, to monitor its development and the state of the containment barriers and the safety functions.

7.4.2.3 The instrumentation shall provide the necessary information to:

- apply the operational control procedures or guides;
- taken the decisions concerning the management of events in the design reference envelope and the design extension conditions.

More specifically, instrumentation shall be provided to determine possible melt-through of the RPV and the presence of hydrogen in the reactor containment.

VII.4.3 Regulation and limitation functions

7.4.3.1 The regulation functions shall be designed to maintain the variables that characterise operation of the installation within the specified normal operating limits.

7.4.3.2 In addition to the regulation functions, limitation functions can be introduced in order, in the event of leaving the normal operating envelope, to help bring the installation back into the envelope; these functions aim in particular at avoiding reaching the protection thresholds that trigger automatic reactor shutdown and activation of the systems fulfilling a safety function for the design-basis conditions.

VII.4.4 Reactor protection system

7.4.4.1 In the design-basis conditions, the reactor protection system shall allow the triggering of automatic measures to protect the reactor, including the automatic reactor shutdown systems, such that the technical acceptance criteria defined in chapter III.3 of this guide are not exceeded. It participates in fulfilling the safety functions under the DEC-A conditions that do not postulate its unavailability.

7.4.4.2 The protection system shall be designed such that it displays very high reliability. The protection system shall belong to the highest nuclear safety class and as such shall satisfy all the recommendations figuring in chapter IV.2.1 of this guide. Particular attention shall be paid to reducing the possibilities of common cause failures.

7.4.4.3 The protection system shall be independent, within the meaning defined in chapter IV.1.2 of this guide, of the systems belonging to a lower safety class. If signals are used jointly by the protection system and by another I&C system, the systems shall be suitably separated from each other and compliance with all the requirements of the protection system shall be verified at the design stage.

7.4.4.4 One of the following events or a combination thereof shall not lead to loss of a function of the protection system:

- a unique failure internal to the protection system or to another system that sends the protection system information required by the protection functions;
- intentionally placing a component or channel of the protection system out of service (for periodic tests or maintenance work, for example).

7.4.4.5 The command signals sent to the actuators by the protection system shall take priority over those sent by the other I&C systems.
Design measures shall to the greatest possible extent prevent inappropriate operator actions that could render the protection system unavailable during normal operation and in incident and accident situations. On the other hand, the protection system shall not prevent the fulfilment of the required manual actions.

7.4.4.6 The design of the protection system shall, save justified exceptions, allow the functionality of a protection system to be tested from the sensor through to input signal injected into the final actuator.

VII.4.5 Control rooms

7.4.5.1 The main control room shall permit operational control of the installation in normal operation and in incident and accident situations, including accidents with core meltdown.
In this respect the main control room shall:

- enable the operators to control reactor operation safely in normal operation. Systems shall be provided to give the operators visual or audio information and to alert them of any operating anomaly that could affect nuclear safety;
- be designed such that the operators are provided with appropriate and sufficient information:
  - to perform a diagnosis of the state of the installation and the effectiveness of the systems involved in the safety functions;
  - to verify the availability of the technical and human resources that are required to intervene to cope with the situation in question;
  - to assess the effects of their actions.

The time frames adopted at the design stage for the operator actions in the control room shall more specifically take into account the complexity and variability of the situations encountered.

7.4.5.2 If computerised operational control means are chosen as the main interface with the operators, their design shall focus particular attention on avoiding the failure modes specific to these means, shall take full advantage of the benefits of these computerised means and shall reinforce the capability of the operating team to carry out the operational control actions.

7.4.5.3 If computerised operational control means are adopted as the main interface with the operators, appropriate measures shall be taken to enable the operating team to control the installation safely in the event of a total or partial failure of these operational control means.
A back-up interface shall be provided for this purpose. This back-up interface shall satisfy requirements of a level that enables all the incidents and accidents that could occur following an initiating event to be managed.
Unavailability of the computerised operational control means shall be detected by a system that is subject to appropriate requirements.

7.4.5.4 Appropriate information displays and management and control means placed in a back-up control room that is physically separate from the main control room shall enable the installation to be brought to and maintained in a safe state should the main control room be out of service. Their design shall be sufficiently similar to those of the main control room for the operators to be able to carry out their actions reliably.
Electrical separation measures shall prevent the events that have put the main control room out of service from rendering unavailable the functions ensured from the emergency control room.

7.4.5.5 The effects of the events in the design reference envelope and the design extension envelope shall be taken into account when defining the measures to implement to ensure the habitability and accessibility of the main control room or, failing this, the back-up control room.

7.4.5.6 Measures shall be taken at the design stage to protect the occupants of the main control room and the back-up control room against ionising radiation due to the accident conditions and the radioactive or hazardous substances released.

VII.5 Emergency management

7.5.1 The emergency situation management premises mentioned in II of article 7.3 of the order of 7th February 2012 shall be designed to withstand the hazards considered in the design extension conditions. The habitability and accessibility of the emergency situation management premises shall be ensured, particularly in the event of an accident with reactor core meltdown and possible associated radioactive releases, including situations affecting several installations on the site simultaneously.
These premises shall be able to:

- accommodate the emergency teams;
- protect and bring aid to the people involved in emergency situation management;
- store all or part of the mobile emergency equipment;
- collect and analyse the data relating to the installation, the meteorology and the environment, necessary for managing the emergency;
- give the alert and communicate the local data necessary for the authorities and off-site emergency services.

Article 7.3 of the order of 7th February 2012

II. - The licensee has emergency situation management premises on or near the site, allowing management of the situation and protecting the personnel involved in the emergency situation. These premises are separate from the installation's usual control rooms, and are designed to be available and accessible, including in the emergency situations.

7.5.2 In particular, the necessary information from the installation in emergency situations[30]:

- to diagnose the state of the installation and monitor the physical systems necessary for its operational control;
- for the public authorities to initiate population protection measures;

shall be available in these emergency situation management premises.

7.5.3 If the management of emergency situations necessitates the use of mobile equipment, including equipment external to the site, connection (access) points shall be installed to enable these means to be used and remain accessible in all the conditions that could be encountered in these situations.

[30] As defined in I of article 1.3 of the order of 7th February 2012 (see definition in appendix 1).

VII.6 Management of radioactive effluents and waste

7.6.1 The quantity and the harmfulness of the radioactive waste produced by the operation and decommissioning of the installation shall be kept to the lowest reasonably achievable level. The following measures shall be implemented in this respect:

- preparation of the waste zoning plan defined by article 6.3 of the order of 7th February 2012 and detailed by ASN resolution 2015-DC-0508 of 21st April 2015 relative to the study of waste management and assessment of the waste produced in the BNIs, especially the study of the mechanisms of radioactive substance dissemination or activation of structures shall be carried out from the installation design stage with a view to limiting the extent and complexity of delimiting the potential nuclear waste production zones and facilitating control of the streams of waste and contaminated equipment;
- the choice of materials used in the installation shall ensure that their properties - especially the chemical properties - are compatible with the phenomena to which they could be subjected. The materials shall moreover be chosen taking account of the radioactive waste management routes so that the volume and harmfulness of the waste produced is kept to the lowest level possible, if necessary after treatment.
  In this respect, the selection of materials aims in particular at:
  - limiting activation, including of any impurities present in the material, especially when the activation products are long-lived;
  - limiting the presence of toxic chemicals, fibrous insulating materials, complexing species or pyrophoric elements in the waste;
  - minimising the dissemination of activated corrosion products;
  - facilitating the decontamination of surfaces;
  - enabling, where applicable and in the context of close-tolerance zoning, certain items of equipment (waste electrical and electronic equipment (WEEE), batteries, etc.) used in potential nuclear waste production zones to receive appropriate protection to prevent them from being contaminated;
- the equipment used in the installation shall be selected so as to minimise the quantity of waste produced during maintenance operations.

7.6.2 The reduction of the quantity and harmfulness of the radioactive effluents produced shall be implemented as part of optimisation approach that includes a detailed assessment of actual experience feedback. This optimisation shall take radiation protection considerations into account.

The following shall be addressed in this context: the characterisation of the substances present in the installation (nature - chemical, radiochemical, biological - quantity);

- the location and routing of the radioactive effluents in the installation;
- at-source limiting of the effluents produced;
- the collection and choice of management route for the different categories of waste and effluents, paying particular attention to the performance of the means of detection, monitoring and measurement of the substances used within the installation;
- consideration of the dilution capacity and the sensitivity of the receiving environment.

7.6.3 Measures shall be taken for the collection, treatment and discharge of the radioactive effluents resulting from normal operation of the installation. The management of the radioactive effluents that could result from incidents or accidents, including with fuel meltdown, should be envisaged as from the design phase.

7.6.4 The design of the systems involved in the management of radioactive effluents and the zones they cross shall take into consideration the risks of loss of integrity of the associated systems.

7.6.5 The radioactive effluent and waste collection, treatment, storage and monitoring systems and the structures that house them shall be able to limit releases of radioactive substances into the environment in the event of internal or external hazards. Their design shall in particular ensure compliance with articles 3.3.2.4.2 and 3.3.3.4.2.

VIII DESIGN DOCUMENTATION

8.1 The documentation concerning the design of the installation and its changes shall be kept up to date during operation of the installation and through to its delicensing.

8.2 It shall be updated to take into account in particular any deviations encountered during construction, in the results of the installation start-up tests and the results of in-service monitoring.

APPENDIX 1

Definitions

Definitions taken from the regulations

Activity important for protection	Activity important for protection of the interests mentioned in article L. 593-1 of the environment code (public security health and safety, protection of nature and the environment), that is to say activities participating in the technical or organisational provisions mentioned in the second paragraph of article L. 593-7 of the environment code, or that could affect them.
Internal hazard, external hazard:	Any event or situation originating respectively inside or outside the basic nuclear installation and that can directly or indirectly lead to damage to elements important for protection or call into question compliance with the specified requirements.
Core	Part of a nuclear fission reactor in which the nuclear fuel is placed and which is designed to permit a nuclear fission chain reaction.
Conservative	Is said of a calculation process or a procedure based on assumptions that increase the effects of the phenomena that can adversely affect the performance of a material, item of equipment or installation and affect nuclear safety or radiation protection.
Criticality	State of a medium in which a nuclear chain reaction sustains itself at a constant level.
Internal failure	Malfunction, failure or damage of an element of the installation or present in the installation, including as a result of inappropriate human action.
Demonstration of nuclear safety	All the elements contained or used in the preliminary safety analysis report and the safety analysis reports mentioned in articles 8, 20, 37 and 43 of the abovementioned decree of 2nd November 2007 and contributing to the demonstration mentioned in the second paragraph of article L. 593-7 of the environment code, which prove that the risks of an accident - radiological or not - and the scale of their consequences are, in view of the current state of knowledge, practices and the vulnerability of the environment of the installation, as low as possible under acceptable economic conditions.

Cliff-edge effect	Sudden change in the behaviour of an installation caused by a slight change in an envisaged accident scenario whose consequences are then seriously aggravated.
Effluent	Any fluid - liquid or gaseous - produced by the installation that could be directly or indirectly released into the receiving medium.
Radioactive effluent	Effluent whose nature, origin or radiological characteristics justify the deployment of measures to protect populations and the environment against the risks or detrimental effects associated with ionising radiation.
Element important for protection (EIP):	Element important for the protection of the interests mentioned in article L. 593-1 of the Environment Code (public security, health and safety, protection of nature and the environment), that is to say structure, equipment, system (programmed or not), hardware, component or software present in a basic nuclear installation or placed under the responsibility of the licensee, fulfilling a function necessary for the demonstration mentioned in the second paragraph of article L. 593-7 of the Environment Code, or checking that this function is ensured.
Initiating event	Internal failure or internal or external hazard that could directly or indirectly cause an incident or accident situation.
Specified requirement	Requirement assigned to an element important for protection so that it fulfils - with the required characteristics - the function provided for in the demonstration mentioned in the second paragraph of article L. 593-7 of the Environment Code, or to an activity important for protection so that it meets its objectives with respect to that demonstration.
Licensee	Natural or legal person operating a basic nuclear installation, whether its situation is in order or not, or having made a creation authorisation application provided for by article L. 593-7 of the Environment Code with a view to operating such an installation.
Organisational and human factors	Factors influencing human performance, such as skills, working environment, task characteristics, and the organisation.

Normal operation	Operation of the installation that includes all the standard states and functions of the installation, including scheduled maintenance or shutdown situations, whether radioactive materials are present or not; also considered as normal operation is any situation defined as such in the demonstration mentioned in the second paragraph of article L. 593-7 of the Environment Code.
Incident or accident	Any event not planned for in normal or degraded mode operation and that could be detrimental to the protection of the interests mentioned in article L. 593-1 of the Environment Code; the potential or actual consequences of an accident are more serious than those of an incident.
Radiation protection	Radiation protection is protection against ionising radiation, in other words all the rules, procedures and prevention and surveillance means aimed at preventing or reducing the harmful effects of ionising radiation caused to people, directly or indirectly, including by their adverse environmental impact.
PWR	Pressurised Water Reactor: nuclear reactor moderated and cooled by light water maintained in liquid state in the core in normal operating conditions by applying appropriate pressure.
Reactivity	In a neutron multiplying medium, relative difference of the effective multiplication factor with respect to 1.
Emergency situation	Radiological emergency situation as defined in article R. 1333-76 of the Public Health Code, or any other situation that could seriously affect the interests mentioned in article L. 593-1 of the Environment Code and requiring an immediate response on the part of the licensee.
Sub-critical	Is said of an medium for which the effective multiplication factor is less than 1.
Hazardous substance	Substance, preparation or mixture that meets the criteria relative to the physical hazards or hazards for health or hazards for the environment defined by the order of 20th April 1994 amended relative to the classification, packaging and labelling of hazardous substances.

Nuclear safety	Nuclear safety comprises all the technical provisions and organisational measures relating to the design, construction, operation, shutdown and decommissioning of basic nuclear installations, as well as the transport of radioactive substance, which are adopted with a view to preventing accidents or mitigating their consequences.
Area where nuclear waste production is possible	Area in which the waste produced is contaminated or activated or likely to be so.

Expressions used in this guide

Aggravating failure[31]	In a safety analysis, the least favourable single failure of an EIP called upon for its beneficial effects during the analysis of an incident, accident or hazard, independently of the initiating event considered. The unfavourable nature is determined with respect to the aim of the analysis.
Design-basis hazard	Internal or external hazard considered in the design reference envelope.
Design-basis condition	The single initiating events (SIE) are grouped so as to define a limited number of design-basis events such that the consequences of each design-basis event encompass those of the corresponding group. The incident or accident transients resulting from this, supplemented by the normal operating conditions, constitute the design-basis conditions.
Single failure criterion	The single failure criterion (SFC) is a deterministic design criterion applicable to certain systems IP; it introduces a requirement for redundancy and independence between the IP equipment item of the system(s) IP that fulfil a safety function with the aim of enhancing the reliability of performance of this function. An system IP is designed in accordance with the single failure criterion if it is capable of fulfilling its safety function despite a single failure affecting one of its equipment items, this failure being independent of the event for which the system IP comes into play.
Single failure	Failure of an item of equipment that is sufficient to prevent that item from fulfilling its expected safety function when required. The failures induced by the failure of this item of equipment form part of the single failure. There are two types of failure: active single failures and passive single failures.

[31] The expression "single failure criterion applied to the demonstration of nuclear safety" is sometimes used in place of the term "aggravating".

Active single failure	An active single failure is characterised by: - an error in the position of a mechanical or electrical equipment item; - the failure of a mechanical or electrical equipment item to respond when a mechanical movement is necessary to fulfil the required function; - the failure of an I&C hardware component leading to non-fulfilment of the required function. Spurious functioning of equipment due to I&C failures is addressed in chapter VII.4.
Passive single failure	A passive single failure is applicable to an item of equipment which does not need to change position to fulfil its required safety function. A passive failure can be, for example: - a leak in the pressurised envelope of a fluid system, with a conventional leakage value[32] until it is isolated. If such a leak affects a pipe and is not detected and isolated, it is assumed to increase until it reaches the flow rate corresponding to a total break; - a mechanical failure preventing the normal flow of a fluid.
Controlled state	Controlled state of a BNI in which sub-criticality, removal of residual power and containment of radioactive substances are ensured in the short term. The term "controlled" means the absence of any rapid unfavourable change in the main parameters characterising fulfilment of the abovementioned functions.
Safe state	Stabilised state of a BNI in which sub-criticality, removal of residual power and containment of radioactive substances are lastingly ensured. The "lasting" nature is assessed in particular with regard to: • the autonomy of the installation and the possibilities of external support; • the possibility of carrying out field work if necessary; • the values and the speed of development of the main parameters characterising the abovementioned functions.
Single initiating event (SIE)	Internal event resulting from a single internal failure.

[32] The basic safety rule RFS 1.3.a, "*Utilisation of the single failure criterion in the safety analysis*", sets this conventional leak at 200 L/min.

Safety function	Function that participates directly in fulfilling one of the fundamental functions mentioned in I of article 3.4 of the order of 7th February 2012.
Support function	Function necessary for the fulfilment of a safety function. Examples of support functions include the supply of electricity, water and thermal conditioning.
Integrity of a barrier	The absence of any irreversible alteration of a barrier calling into question the effectiveness provided for in the demonstration of nuclear safety.
Analysis method	Procedure defining certain assumptions (initial and limit conditions etc.), consideration of uncertainties, penalties, calculation methods and calculation sequences necessary for the analysis in point, consistently with the rules of the demonstration of nuclear safety.
Reasonably practicable	The reasonably practicable (or on the contrary, not reasonably practicable) nature of a measure or the achieving of an objective is assessed on the basis of an overall balance of the gains in safety and radiation protection compared with the drawbacks, particularly with respect to the industrial, economic aspects and the complexification of the design or future operation in view of the state of the techniques and the stage of project development. As a general rule, this assessment implies examining different solutions in due time.
Plausible situation	A situation (initiating event or combination of initiating events) is considered plausible if its estimated frequency of occurrence is sufficiently high or its possibility of occurrence is sufficiently credible for it not to be ignored in the demonstration of nuclear safety with respect to the objectives mentioned in 2.1.2.3.

APPENDIX 2
Correspondence with the terminology used in the international texts (IAEA, WENRA)

International terminology (IAEA, WENRA)	Terminology used in the guide	*Comments*
Design Basis Accident (DBA)	**Design-basis conditions of categories 3 and 4**	
Operational states + DBA	**Design-basis conditions**	
Operational states + DBA + internal & external hazards	**Design reference envelope**	The design reference envelope covers the design-basis internal and external hazards for which there is no clearly identified international terminology. WENRA nevertheless recommends the identification of a "design-basis event" for the natural hazards.
Design Extension Conditions (DEC)	**Design extension envelope**	The design extension envelope used in this guide is equivalent to WENRA's DEC. The DEC terminology of the IAEA does not consider hazards which are qualified as "Beyond Design Basis External Event". The approaches of the IAEA and of this guide nevertheless remain coherent despite this difference in terminology.
Accident conditions	**Design-basis conditions of category 3 and 4 + DEC-A + DEC-B**	
Postulated initiating event (PIE)	**Postulated initiating event**	In this guide the initiating events include hazards, whereas the international texts leave room for interpretation in this respect.

APPENDIX 3
RFS (basic safety rules) and ASN guides applicable on the date of publishing of this document

The following table presents the basic safety rules (RFS) and ASN guides whose principles are applicable.

In view of the tightened recommendations for the new-generation pressurised water reactors, this document - in certain respects - presents different approaches to those figuring in the RFS's and guides mentioned in the table below, the majority of which were developed when the original PWRs were designed and apply to the installations currently in operation. These RFS's and guides may thus necessitate adaptations in their application. Whatever the case, the recommendations indicated in this document take precedence for the new reactors.

Reference of the RFS or Guide	Subject
RFS I.2.a of 5/08/1980	Integration of risks related to aircraft crashes
RFS I.2.b of 5/08/1980	Integration of risks of projectile release following fragmentation of the turbogenerators
RFS I.3.a of 5/08/1980	Use of the single failure criterion in safety analyses
RFS I.2.a of 7/05/1982	Integration of risks related to the industrial environment and communication routes
RFS I.1.a of 10/06/1982	Meteorological measurement means
RFS I.3.a of 08/06/1984	Seismic instrumentation
RFS IV.2.b of 31/07/1985	Requirements to be considered in the design, qualification, implementation and operation of electrical equipment included in safety-classified electrical systems
RFS I.3.c of 01/08/1985	Geological and geotechnical site studies; determination of soil characteristics and study of soil behaviour
RFS V.2.e of 25/10/1985	General rules applicable to the production of fuel assemblies
RFS II.4.1.a of 15/05/2000	Software for safety-classified electrical systems
RFS 2001-01	Determination of the seismic risk for the safety of the installations
ASN Guide /guide/2/01	Integration of the seismic risk in the design of BNI civil engineering structures
RFS 2002-01 of 26/12/2002	RFS relative to the development and utilisation of probabilistic safety assessments (PSA)
ASN Guide No. 6	Final shutdown, decommissioning and delicensing of basic nuclear installations
ASN Guide No. 13	Protection of basic nuclear installations against external flooding
ASN Guide No. 14	Clean-out of structures in basic nuclear installations

APPENDIX 4

List of acronyms

	International Atomic Energy Agency
ASN	*Autorité de sûreté nucléaire* - French nuclear safety authority
DBC condition	Design-basis condition
DEC-A condition	Design extension condition (for which fuel meltdown is prevented)
DEC-B condition	Design extension condition (for which fuel meltdown is postulated)
DT	Technical guidelines for the design and construction of the new-generation pressurised water nuclear reactors
EIP	Element Important for Protection
SIE	Single Initiating Event
PSA	Probabilistic Safety Assessment
GP ESPN	Advisory Committee of Experts for Nuclear Pressure Equipment
GPR	Advisory Committee of Experts for Nuclear Reactors
BNI	Basic Nuclear Installation
IRSN	*Institut de radioprotection et de sûreté nucléaire*
PWR	Pressurised Water Reactor
RFS	*Règle fondamentale de sûreté* - Basic safety rule
WENRA	Western European Nuclear Regulators' Association

15-21, rue Louis Lejeune
92120 Montrouge

Telephone +33 (0)1 46 16 40 16
Fax (+33) 1 46 16 41 47