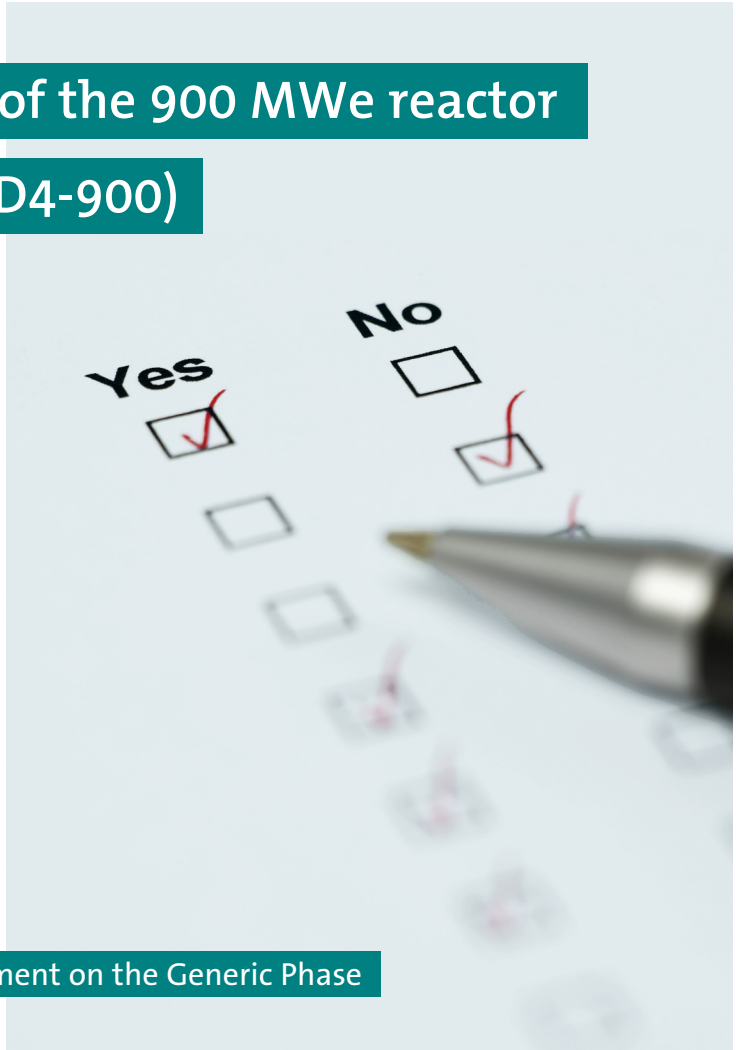
ENVIRONMENT AGENCY AUSTRIA umweltbundesamt

Review of the 900 MWe reactor Fleet (VD4-900)



Expert Statement on the Generic Phase

Federal Ministry
Republic of Austria
Sustainability and Tourism

ENVIRONMENT AGENCY AUSTRIA umweltbundesamt

REVIEW OF THE 900 MWE REACTOR FLEET (VD4-900)

Expert Statement on the Generic Phase

Oda Becker
Martin Giersch
Franz Meister
Manfred Mertins
Geert Weimann

By Order of the Federal Ministry for Sustainability and Tourism
Directorate I/6 General Coordination of Nuclear Affairs
BMNT: BMNT-UW.1.1.2/0019-I/6/2018

Federal Ministry
Republic of Austria
Sustainability and Tourism

REPORT
REP-0686

Vienna, 2019

Project management

Franz Meister *(Umweltbundesamt)*

Authors

Franz Meister, Martin Giersch *(Umweltbundesamt)* – Introduction

Oda Becker – Core Melt Accidents & Spent Fuel

Manfred Mertins – Accidents without core melt, Internal/external hazards, Implementation of necessary upgrades in time

Geert Weimann – Upgrade Implementation Compliance

Layout and typesetting

Elisabeth Riss *(Umweltbundesamt)*

Title photograph

© iStockphoto.com/imagestock

For further information about the publications of the Umweltbundesamt please go to: http://www.umweltbundesamt.at/

Imprint

Owner and Editor: Umweltbundesamt GmbH
Spittelauer Lände 5, 1090 Vienna/Austria

The Environment Agency Austria prints its publications on climate-friendly paper.

ISBN 978-3-99004-505-3

CONTENT

SUMMARY

Électricité de France (EdF) intends to get a licence for the prolonged operation of its 900 MW nuclear power plant fleet beyond 40 years of operation. This project is subject to a voluntary public consultation process, initiated by the High Committee for Transparency and Information on Nuclear Safety (HCTISN).

The Federal Environmental Agency commissioned an expert statement to conduct an assessment of the documents publicly available for the Federal Ministry for Sustainablity and Tourism.

The Expert Statement is based on these documents, in particular the Fulfillment Report and other publicly available studies and reports related to the 900 MW reactor fleet.

Current relevant requirements, at international as well as European level have been compared with the measures intended by EdF. Main focus was on EdF´s objective to upgrade the reactors to a safety level comparable to the EPR.

The Experts' Statement does not intend to address all relevant safety aspects related to the lifetime extension of the 900 MW reactor fleet, but focuses on those topics raised by EdF itself.

As also for the French 900 MW nuclear reactors severe accidents with significant releases of radioactive substances, which could cause intervention measures in Austria, cannot be excluded, Austria considers itself as a concerned party.

The experts consider that the following conditions must be met as a prerequisite for life-time extension of a 900 MW NPP of the French CP0/CPY generation:

- Proof of compliance with the required safety margins over the intended service life extension, especially for the components designed for service life of 40 years only (without the use of probabilistic analysis results as proof).
- All retrofits considered necessary to meet the safety objective – adaptation to the safety features of the EPR – shall be performed before re-commissioning after the 4th safety review, in particular:
  - Consistent separation of the operational and the safety-related functions of the affected systems.
  - Increased redundancy of safety systems, including the safety-relevant supply systems
  - Ensuring the independence of the individual redundancies of the safety systems, even with the respectively designated safety-relevant supply systems.
  - Proof of event-control of events classified as PCC-2 (Reference transients), PCC-3 (Reference incidents) and PCC-4 (Reference accidents) regarding the EPR.
  - Increasing the functional resistance of the safety-relevant facilities, even against extreme (beyond design basis) external influences and impacts (earthquake, plane crash ...). Here the structural plant components are of particular importance.
- Complete safety level 4 functional compliance of the plants, in particular:

- Complete installation of the “Hard Core” as a system of safety level 4a.
- Proof of control of the plant conditions classified as RRC-A (Risk Reduction Category A) comparable with the EPR provisions (without the use of results of probabilistic analysis only).
- Accident management measures shall also be available in the case of extreme external impacts. Their availability and survivability over a longer period is important.
- Exclusion of cliff edge effects, even in the case of extreme internal and external impacts.
- Proof of the EPR's RRC-B (Risk Reduction Category B) classification of core meltdown phenomena with regard to the ability of the concept to limit the release of radioactive material into the environment – level of defence 4b (without use of results of probabilistic analysis only). This is to proof for all modifications to be introduced into the French CP0/CPY vintage plants.

After performing the PLE program, a considerable gap between the safety level of the 900 MW reactor and the EPR will persist. For VD4-900 review, the overall objective is to avoid melting of the fuel and limit radioactive releases in all respects consistent with the precautions introduced for the EPR. However, the safety requirements to reach the related goals are only partly addressed by EDF’s proposals. The plants cannot demonstrate that design basis accidents (DBA) can be handled according to safety standards valid for reactors in operation.

The scope of the PLE program concerning core melt accidents is not in compliance with current safety requirements. The same applies for the demonstration of safety. A failure of the containment function cannot be excluded after implementation of the envisaged modification for the stabilization of the molten core and for containment heat removal.

The Hardened Safety Core (HSC) that shall have an important role for the prevention of core melt accidents, but also for the mitigation of the consequences of core melt accidents, is not implemented yet. Furthermore, after complete implementation, it is not assured that the HSC (and in particular the existing structures, systems and components (SSC) of the HSC) will meet the safety requirements to their full extend.

For the 900 MW reactors, a core melt accident with a major release is possible today and this will also be possible after the implementation of the currently envisaged PLE program.

Spent Fuel Pool

The stress tests have revealed several weaknesses of the safety level for the spent fuel storage pools of the 900 MWe reactors. Most of the required backfittings measures are not implemented yet.

However, the most dangerous weakness, the vulnerability of the SFP, because of the thin walls, will remain for the next 20 years. Improvements are not envisaged in the PLE program. Thus, the 900 MW reactors will not meet the safety standards requirements similar to the EPR (protection of the spent fuel building against a crash of the commercial airplane).

An external event that led to a leakage in the spent fuel pool of the 900 MW reactors would cause the loss of the cooling water. Because sufficient provisions to refill the pool water are not in place an unavoidable severe accident would occur with considerable releases of radioactive substances.

ZUSAMMENFASSUNG

Électricité de France (EdF) strebt die Bewilligung für den Weiterbetrieb der 900 MW Reaktorflotte über die angenommene 40 jährige Betriebsdauer hinaus an.

Das High Committee for Transparency and Information on Nuclear Safety (HCTISN) hat ein – auf freiwilliger Basis stattfindendes – öffentliches Begutachtungsverfahren eingeleitet

Ein Expertenteam unter der Leitung des Umweltbundesamtes hat für das Bundesministerium für Nachhaltigkeit und Tourismus eine Fachstellungnahme zum französischen Konsultationsprozess bezüglich die generischen Anforderungen an die Betriebsverlängerung der französischen 900 MW-Kernkraftwerke erarbeitet.

Grundlage der Fachstellungnahme sind die im französischen Verfahren veröffentlichten Unterlagen, insbesondere die Zusammenfassung des sogenannten Fullfillment Report der Betreiberfirma EdF, wie auch andere öffentlich zugängliche Studien und Berichte zur 900 MWe-Kraftwerksflotte. Die aktuell gültigen Anforderungen des internationalen, insbesondere des EU-Regelwerkes an Kernkraftwerke wurden vor dem Hintergrund des Anspruches der Betreiberfirma EdF geprüft, die ein Sicherheitsniveau für diese Reaktoren anstrebt, das jenem des EPR entsprechen soll.

Die vorliegende Fachstellungnahme hat nicht den Anspruch, alle relevanten Themenbereiche zu behandeln, die sich mit der Frage der Laufzeitverlängerung verbinden, sondern fokussiert vor allem auf die von EdF selbst angeführten Themen.

Die Betroffenheit Österreichs ergibt sich daraus, dass auch für die französischen 900 MW Kernreaktoren schwere Unfälle mit bedeutenden Freisetzungen an radioaktiven Stoffen nicht ausgeschlossen werden können und in einem solchen Fall Interventionsmaßnahmen in Österreich erforderlich werden können.

Die Experten sind der Auffassung, dass die folgenden Bedingungen als Voraussetzung für eine Laufzeitverlängerung eines 900 MW AKW der französischen CP0 und CPY Generationen erfüllt sein müssen:

- Nachweis der Einhaltung der erforderlichen Sicherheitsreserven über die beabsichtigte Lebensdauerverlängerung insbesondere für die Komponenten, die nur für eine Laufzeit von 40Jahren ausgelegt sind (ohne Zuhilfenahme probabilistischer Analyseergebnisse).
- Alle zur Erreichung der sicherheitstechnischen Zielsetzung – Anpassung an die Sicherheitsmerkmale des EPR – als erforderlich angesehenen Nachrüstungen sind vor Wiederinbetriebnahme nach der 4. Sicherheitsüberprüfung durchzuführen, insbesondere:
  - Konsequente Trennung betrieblicher von sicherheitstechnischen Funktionen bei den jeweils betroffenen Systemen.
  - Erhöhung des Redundanzgrades der Sicherheitssysteme, einschließlich der sicherheitstechnisch wichtigen Versorgungssysteme.
  - Gewährleistung der Unabhängigkeit der einzelnen Redundanzen der Sicherheitssysteme einschließlich der der jeweils zugeordneten sicherheitstechnisch wichtigen Versorgungssysteme.

  - Nachweis der Beherrschung der beim EPR als PCC-2 (Reference transients), PCC-3 (Reference incidents) und PCC-4 (Reference accidents) klassifizierten Ereignisse.
  - Ertüchtigung der sicherheitstechnisch wichtigen Einrichtungen hinsichtlich der Widerstandsfähigkeit auch gegen extreme (auslegungsüberschreitende) externe Einwirkungen (Erdbeben, Flugzeugabsturz …). Den baulichen Einrichtungen kommt hier eine besondere Bedeutung zu.
- Aufbau eines vollständigen Ebene 4 Konzepts, insbesondere
  - Vollständige Installation des „Hard Core“ als System der Sicherheitsebene 4a (Notstandssystem).
  - Nachweis der Beherrschung der beim EPR als RRC-A (Risk Reduction Categorie A) klassifizieren Anlagenzustände (ohne ausschließliche Berücksichtigung der Ergebnisse aus den PSA-Untersuchungen).
  - Maßnahmen und Einrichtungen des anlageninternen Notfallschutzes sollen auch bei extremen externen Einwirkungen verfügbar sein. Dabei ist deren Verfügbarkeit über einen längeren Zeitraum von Bedeutung.
  - Ausschluss von cliff-edge Situationen für den Fall extremer Einwirkungen.
  - Nachweis der beim EPR als RRC-B (Risk Reduction Categorie B) klassifizieren Kernschmelzphänomene hinsichtlich einer Begrenzung der Freisetzung radioaktiver Stoffe in die Umgebung – Sicherheitsebene 4b (ohne ausschließliche Berücksichtigung der Ergebnisse aus den PSA-Untersuchungen).

Nach der Durchführung des PLE-Programms bleibt eine erhebliche Lücke zwischen dem Sicherheitsniveau des 900-MW-Reaktors und dem EPR bestehen. Das Gesamtziel für die Überprüfung des VD4-900, d.h. die Vermeidung einer Kernschmelze und die Begrenzung der radioaktiven Freisetzung, steht im Einklang mit den für den EPR verwendeten Sicherheitszielen. Die Sicherheitsanforderungen zur Erreichung dieses Ziels werden jedoch nur teilweise erfüllt.

Der Umfang des PLE-Programms bezüglich Kernschmelzunfällen entspricht nicht den aktuellen Sicherheitsanforderungen. Gleiches gilt für den Nachweis der Sicherheit. Ein Ausfall der Containment-Funktion kann nach Durchführung der vorgesehenen Modifikation zur Stabilisierung des geschmolzenen Reaktorkerns und zur Wärmeabfuhr des Containments nicht ausgeschlossen werden.

Der sogenannte Hardened Safety Core (HSC), der eine wichtige Rolle bei der Vermeidung von Kernschmelzunfällen, aber auch bei der Minderung der Folgen von Kernschmelzunfällen spielen soll, ist noch nicht implementiert. Darüber hinaus ist nicht sichergestellt, dass der HSC (und insbesondere die bestehenden Strukturen, Systeme und Komponenten (SSC) des HSC) nach vollständiger Implementierung ausreichende Sicherheitsanforderungen erfüllen werden.

Für die 900-MW-Reaktoren ist heute ein Kernschmelzunfall mit einer großen Freisetzung möglich und wird auch nach der Umsetzung des derzeit geplanten PLE-Programms möglich sein.

Im Zuge der EU-Stress Tests wurden zahlreiche Schwachstellen bezüglich der Brennelementlagerbecken der 900 MW-Reaktorflotte offensichtlich. Viele vorgeschriebene Nachrüstmaßnahmen wurden bislang noch nicht abgeschlossen.

Die bedeutendste Schwachstelle stellt die Verwundbarkeit der Brennelementlagerbecken selbst dar, welche nur durch relativ dünn ausgeführte Wände geschützt sind. Diese Gefährdungslage würde weitere 20 Jahre bestehen, zumal Maßnahmen zur Behebung dieser Schwachstelle derzeit nicht vorgesehen sind. Das Programm zur Betriebsverlängerung wird daher nicht das selbstgesteckte Sicherheitsziel erreichen können, da hier die Anforderungen, wie sie für den EPR bestehen, insbesondere Schutz der Brennelementlagerbecken gegen einen Flugzeugabsturz, nicht erreicht werden wird können.

Ein extern induzierter schwerer Unfall in einem Brennelementlagerbecken der 900 MW-Reaktoren kann so zu einem Kühlmittelverlust führen. Ausreichende Maßnahmen zur Sicherstellung der notwendigen dauerhaften Wasserbedeckung sind derzeit nicht verfügbar.

1 INTRODUCTION

1.1 General Comments regarding the public consultation process

The Experts welcome the decision of the High Committee for Transparency and Information on Nuclear Safety (HCTISN) to conduct a public consultation on the occasion of the 4th periodic safety review of France's 900 MWe nuclear power reactors, with a view to involve the general public in decisions regarding the life extension of these reactors beyond 40 years of operation.[1]

This procedure will cover topics beyond legislative requirements such as the energy transition for green growth, passed on 17 August 2015, demanding a systematic public enquiry into the arrangements put forward by the licensee for the life extension of its nuclear reactors after 35 years of operation."

The Experts appreciate the opportunity to participate in the public consultation's prolonged discussion period which provides an instrument to extend its scope to include all topics covered by the review and by opening the exchange of views up to a wider audience.

The Experts propose to be further involved in the process in a first step for the consultation regarding generic aspects noting to consider also taking part in the second phase conducted to site specific consultations as far as relevant, guided by the set of principles established by the HCTISN as aligned with the general framework of public information and consultation defined by article L. 120-1 of the environment code.

1.1.1 Relevance for Austria

The public consultation is relevant for Austria, as consequences above intervention levels from Severe Accidents can be not excluded (SA) also from French Nuclear Sites on Austrian territory, considering even their low probability.

Depending on meteorological conditions the French 900 MW PWR nuclear plants of Tricastin (units 1, 2, 3, 4), Cruas Meysse (units 1, 2, 3, 4), Bugey (units 2, 3, 4, 5), Fessenheim (units 1, 2) and Dampierre (units 1, 2, 3, 4) are certainly relevant under severe accident consequences, if dominant west wind weather conditions and source terms related to beyond design basis accidents are assumed. Because source terms have not been published in detail by any nuclear reactor operators in Europe, it cannot be excluded, that large releases can occur and can result in depositions above valid intervention levels under certain weather conditions. [2]

[1] https://concertation.suretenucleaire.fr/pages/public-consultation-on-safety-enhancements-to-frances-fleet-of-900-mwe-reactors-on-the-occasion-of-their-4th-periodic-safety-review

[2] http://flexrisk.boku.ac.at/en/evaluationCountryExport.phtml#form

"The project flexRISK studies the geographical distribution of the risk due to severe accidents in nuclear facilities, especially nuclear power plants (NPP) in Europe. Starting with source terms and accident frequencies, the large-scale dispersion of radionuclides in the atmosphere were simulated for about 2,800 meteorological situations. Together with the subsequent calculation of resulting radiation doses the consequences of severe accidents can be estimated. Maps and diagrams will indicate, e.g., where in Europe the risk to be affected by a severe accident is especially high, or which contribution is incurred by the NPPs of a specific country." [3]

The Flexrisk Project also calculated the risk originated from French NPPs. The results demonstrated, that depositions (e.g. Cs-137) above intervention levels cannot be excluded per se.

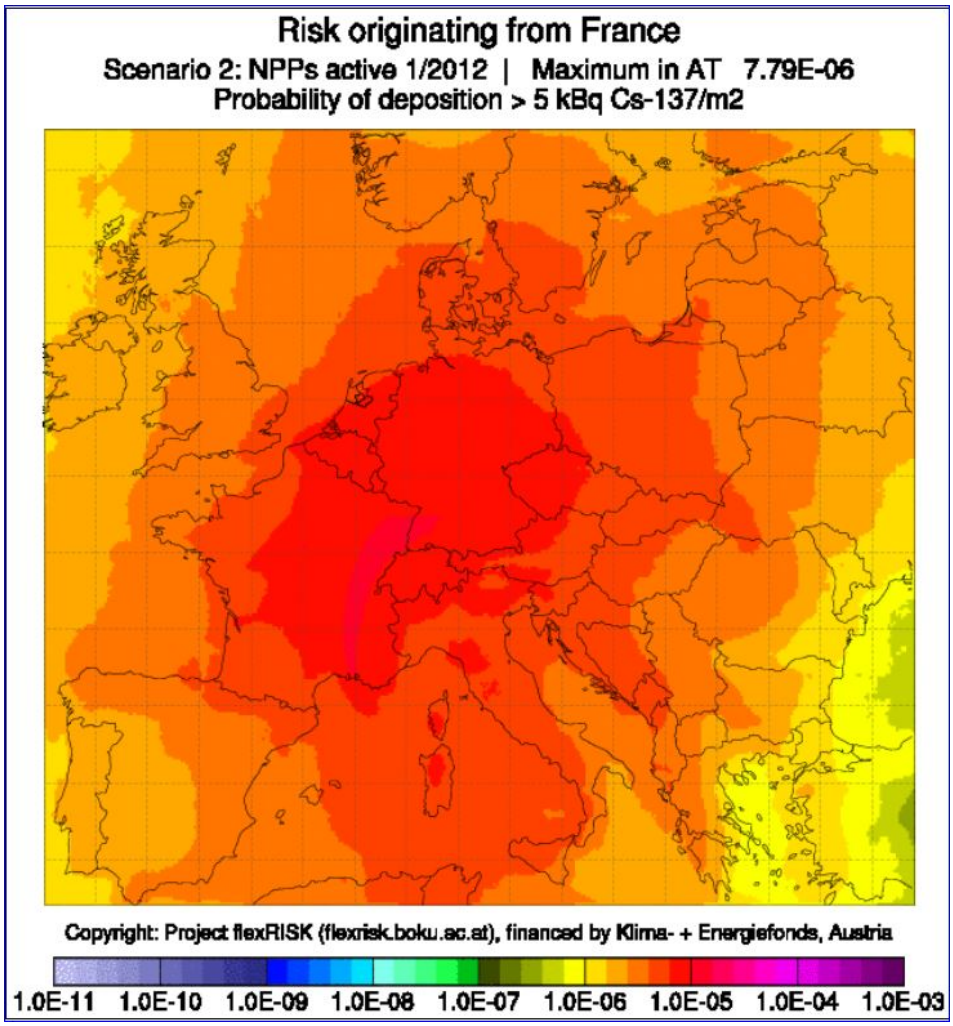


Figure 1: Risk originating from France. (http://flexrisk.boku.ac.at/en/evaluationCountryExport.phtml#form)

[3] http://flexrisk.boku.ac.at/en/index.html

In 2013, IRSN conducted a study to estimate the cost of accidents in nuclear power plants.[4] This study estimated the contaminated area affected by radioactivity release of aerosol discharges of a major accident at about 10 E+15 to 10 E+19 Bq of about 18.800 km[25]

In 2014 the HERCA-WENRA working group published its approach for an enhanced and harmonisedcross-border coordination of protective actions during the early phase of a nuclear accident. It was mentioned that „*Fukushima has shown again that a severe nuclear accident anywhere in the world, including Europe, cannot be completely excluded. Considering the safety level of European nuclear power plants and their improvements resulting from the lessons learned from various events (including the Fukushima disaster), it is estimated that the probability of such a severe accident is very low. But, as improbable such an accident might be, EP&R arrangements must be prepared for such cases, too.*“[6]

Based on the findings of the Flexrisk Project, IRSN studies and the HERCA-WENRA working group results on Severe Accidents in nuclear facilities, Austria may be affected by the operation of NPPs, mainly those, where measures to avoid large releases of radioactivity in case of accidents cannot be excluded.

Concerning the ongoing procedure it is of importance to point out, that “Severe accidents were not considered at the design stage of the generation II French PWRs.”[7]

1.2 Requirements and Obligations

Austria would like to underline the necessity to consequently fulfil the entire legal and regulatory framework when deciding under which conditions the French 900 MWe 3-loop PWR generation II reactors should get authorisations to be operated beyond the time frame originally intended.

It is of immanent importance for the 4th Periodic Safety Review to analyse and ensure completeness and extent of the objectives and approach against valid legal requirements and obligations also from EU/Euratom and international in-

[4] (IRSN 2013) Methodology applied by IRSN to estimate costs of nuclear accidents in France, CRI-report PRP / CUSSU / 2013-00261

[5] (IRSN 2013) The activity released by radioactive aerosols is a physical indicator of the severity of releases. The EPS2 clarifies that it varies in the case of the 900 MWe reactors, the most numerous of the park, levels below 10 15 Bq to levels 10 19 Bq or more, a ratio of more than 1 to 10 000. and (IRSN 2013) page 40

[6] http://www.herca.org/docstats/HERCA-WENRA%20approach%20for%20better%20cross-border%20coordination.pdf

[7] (IRSN 2015) Past and Future R&D at IRSN on Corium Progression and Related Mitigation Strategies in a Severe Accident; Didier Jacquemain, Didier Vola, Renaud Meignen, Jean-Michel Bonnet, Florian Fichot,Emmanuel Raimond, Marc Barrachin -Institut de Radioprotection et de Sûreté Nucléaire (IRSN) in : Proceedings NURETH-16, Chicago, IL, August 30-September 4, 2015

struments and also on technical level of the four main safety-related topics[8] as proposed by EdF[9]:

1. Accidents without core melt
2. Internal/external hazards
3. SF-pool
4. Core melt accidents.

Already before the Fukushima Dai-ichi nuclear accidents, international instruments were in place establishing safety obligations for existing nuclear power plants including initiating and review of continuous safety improvements, also relevant for all four topics for French nuclear installations.

The international nuclear safety framework was revised and further strengthened, incorporating lessons learned from Fukushima nuclear accidents and recognizing challenges from the ageing nuclear fleet with increasing needs for safety upgrades in case of Long Term Operation (LTO), especially beyond the design life span as originally intended during initial project development and licensing.

Euratom Members States are obligated to transpose basic requirements into national legislation and regulatory framework, as defined under the Euratom Nuclear Safety Directive[10], which was revised in 2014[11] to address post Fukushima requirements.

The revised Directive defines in Article 8a "Nuclear safety objective for nuclear installations":

1. *Member States shall ensure that the national nuclear safety framework requires that nuclear installations are designed, sited, constructed, commissioned, operated and decommissioned with the objective of preventing accidents and, should an accident occur, 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 radioactive releases that would require protective measures that could not be limited in area or time.

More specific with regard to existing nuclear power plants the Directive states:

2. *Member States shall ensure that the national framework requires that the objective set out in paragraph 1:*

   …
   (b) is used as a reference for the timely implementation of reasonably practicable safety improvements to existing nuclear installations, including in the framework of the periodic safety reviews as defined in Article 8c(b).

[8] For more on the topics, see below.

[9] Summarised version of the fulfilment report VD4-900, 2018

[10] Council Directive 2009/71/Euratom of 25 June 2009 establishing a Community framework for the nuclear safety of nuclear installations

[11] Council Directive 2014/87/Euratom of 8 July 2014 establishing a Community framework for the nuclear safety of nuclear installations

ENSREG[12] invited WENRA[13] to develop guidance to interpret key elements of the Directive. WENRA provided therefore "*Guidance on Article 8a of the* (revised) *EU Nuclear Safety Directive*[14] on *"Timely Implementation of Reasonably Practicable*[15] *Safety Improvements to Existing Nuclear Power Plants"* mentioning technical concepts to support transposition and implementation of the Directive with main focus on application to NPPs.

The issue is of specific relevance for nuclear installations which are planned to undergo a safety assessment for licensing/permission of operation beyond the original design lifetime in Long Term Operation (LTO) as it is foreseen for most of the French PWR 3-loop plant fleet based on the 4th Periodic Safety Review for a further 10-year operation interval beyond plant age of more 40 years.

WENRA issued the topics to be addressed for existing NPPs referring to safety requirements for new NPP to identify and prioritize safety improvements and its timely implementation on plant and organisational level.

WENRA reported its approach in a "*Framework for implementation of "reasonably practicable" improvements*" which is structured into main topics and drivers of safety improvements also proposing adequate methodologies and instruments, including the defence in depth (DiD) concept, the role of probabilistic safety analysis (PSA), equivalence of outcomes and proportionality of assessment results, adequate decision making process, consideration of economic aspects (role of cost) and concepts for "timely implementation" of safety improvements.

The revised WENRA *Safety Reference Levels (SRLs) for existing NPPs*[16] take lessons learned from Fukushima nuclear accidents and provide a systematic frame to continuously improve nuclear safety. From 19 Topical Issues at least 5 are explicitly dealing with technical aspects of safety enhancements and reference to requirements for new nuclear power plants in the context of LTO and ageing management. The SRLs concluded, that long term operation has not only to address ageing in terms of physical degradation of Structures, Systems and Components (SSCs) but also requires to compare the safety concepts on level of fulfilment of safety functions with state-of-the-art technological solutions, identifying possible gaps and developing back-fitting measures to comply as far as reasonable practicable. All steps have to be implemented based on a com-

[12] European Nuclear Safety Regulators Group

[13] Western European Nuclear Regulators Association

[14] WENRA Guidance on Article 8a of the EU Nuclear Safety Directive: "Timely Implementation of Reasonably Practicable Safety Improvements to Existing Nuclear Power Plants", Report of the Ad-hoc group to WENRA, 13 June 2017, http://www.wenra.org/media/filer_public/2017/07/13/wenra_guidance_on_article_8a_of_nsd_to_ensreg.pdf

[15] COMMENT: the acceptance of the term reasonably practicable implies an evaluation of safety measures to be adopted in the light of the residual life assumption related to the specific nuclear installation, whereas the "´reasonably achievable" attribute appears to be more adequate, while it cannot by tied to concepts dominated by residual risk determination in a balancing effort. (Permissible reduction of safety margins at the EOL of the installation can be accepted…).

[16] WENRA Safety Reference Levels for Existing Reactors.UPDATE IN RELATION TO LESSONS LEARNED FROM TEPCO FUKUSHIMA DAI-ICHI ACCIDENT. 24th September 2014 http://www.wenra.org/media/filer_public/2016/07/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf

prehensive and covering update of the safety analysis, actual plant status and requirements for new facilities in force.

Most important topical Issues following the structure of the revised WENRA SRLs dealing with re-evaluation of the design basis and plant safety capabilities are:

- Issue E: Design Basis Envelope for Existing Reactors
- Issue F: Design Extension of Existing Reactors
- Issue G: Safety Classification of Structures, Systems and Components
- Issue LM: Emergency Operating Procedures and Severe Accident Management Guidelines

The following topical Issues are concentrated on assessment methodologies relevant in this regard:

- Issue J: System for Investigation of Events and Operational Experience Feedback
- Issue N: Contents and Updating of Safety Analysis Report (SAR)
- Issue O: Probabilistic Safety Analysis (PSA)
- Issue P: Periodic Safety Review (PSR)

Safety Cases and plant conditions including ageing aspects and site re-evaluation are elaborated mainly under:

- Issue I: Ageing Management
- Issue R: On-site Emergency Preparedness
- Issue S: Protection against Internal Fires
- Issue T: Natural Hazards

Overlaps in this classification have to be considered. Selected Safety Reference Levels regarding safety improvements establishes requirements in higher but still generic detail are presented under:

Issue E2. defines the Safety Strategy by application of Defence in Depth (DiD) principles:

"The design shall prevent as far as practicable:

- *challenges to the integrity of the barriers;*
- *failure of a barrier when challenged;*
- *failure of a barrier as consequence of failure of another barrier."*

Issues E11.1 deals with the *"Review of the design basis: The actual design basis shall regularly, and when relevant as a result of operating experience and significant new safety information, be reviewed, using both a deterministic and a probabilistic approach as well as engineering judgement to determine whether the design basis is still appropriate. Based on the results of these reviews needs and opportunities for improvements shall be identified and relevant measures shall be implemented."*

Issue F1. defines the *"Objectives for Design Extension Conditions"* (DEC) for existing reactors by:

- *"enhancing the plant's capability to withstand more challenging events or conditions than those considered in the design basis,*

- *minimising radioactive releases harmful to the public and the environment as far as reasonably practicable, in such events or conditions.",*

applicable for events without and with fuel damage.

Guidance for the selection of DEC is provided under F2 providing a list of requirements to be fulfilled for safety analysis of DEC including deterministic and probabilistic approach also taking into account Severe Accident phenomena and detailing the conditions under which the safety functions has be ensured and with the possibility of defined review activities.

Issue F5. sets up Reference Levels for the *"Review of the design extension conditions"*

Issue I on Ageing Management establish technical recommendations directly applicable under VD4 for the PWR 900 MW_e fleet:

- Ageing of key structures, systems and components (SSCs) such as reactor vessel or reactor containment, is a common limiting factor for LTO.
- Address safety level of the NPP and possibilities for safety improvements.
- SRL I2.2: The licensee shall provide monitoring, testing, sampling and inspection activities to assess ageing effects to identify unexpected behaviour or degradation during service.
- SRL I3.1: Ageing management of the reactor pressure vessel and its welds shall take all relevant factors including embrittlement, thermal ageing, and fatigue into account to compare their performance with prediction, throughout plant life.
- SRL I3.2: Surveillance of major structures and components shall be carried out to timely detect the inception of ageing effects and to allow for preventive and remedial actions.

Issue P3. provides guidance on the *"Methodology of the periodic safety review" (PSR).* Key objectives of PSR are under revised RLs:

- Confirmation of compliance of NPPs with licensing basis (P1.2)
- Identification and timely implementation of reasonably practicable improvement measures (P1.4)
- Identification of issues that might limit the lifetime of the facility (P1.5)
- Use of an up to date, systematic, and documented methodology (deterministic and probabilistic) (P3.1)
- P1.3 states explicitly: *"The review shall identify and evaluate the safety significance of deviations from applicable current safety standards and internationally recognised good practices taking into account operating experience, relevant research findings, and the current state of technology."*
- P3.2 request to *"…identify what safety improvements are reasonably practicable."*

"Considerations for events more severe than the design basis events" is requested under Issue T6.

The conducted overall review of the SRLs took also into account of new IAEA publications and safety development.

The WENRA Pilot Study on LTO still could not include lessons learnt from Fukushima but already defined requirements on LTO and ageing management[17].

In response to the 2011 Fukushima nuclear accident, risk and safety assessments ('stress tests') were carried out on all nuclear power plants in Euratom Member States. "*The aim of the assessments was to check whether the safety standards used when specific power plants received their licences were sufficient to cover unexpected extreme events. Specifically, the tests measured the ability of nuclear facilities to withstand damage from hazards such as earthquakes, flooding, terrorist attacks or aircraft collisions.*"[18]

France participated in the Stress Test peer review process to the full extent and presented together with the follow-up results a detailed National Action Plan (NAcP) for safety based on recommendations[19]

Outcomes of the first Topical Peer Review on Ageing Management required under the revised Nuclear Safety Directive were presented by ENSREG in October 2018 and identified also for France´s topics of improvement[20].

During its meeting in fall 2017, WENRA recognised work which was performed by its Reactor Harmonisation Working Group (RHWG) on the implementation of the 2014 RLs underlining the need for timely implementation of reasonably practicable improvements on nuclear power plants including implementation of VDNS[21] Principle 2 and implementation of NSD articles, especially 8(a)[22].

At the June 2015 ENSREG conference, regarding "Safety Requirements for Long Term Operation or Ageing Aspects and for Design, Construction and Operation of New Nuclear Power Plants"[23] the WENRA chair underlined the link between the revised SRLs for existing and the Safety Objectives for new Nuclear Power Plants referring also to the WENRA Report on Safety of new NPP designs from March 2013.

The Compilation of Recommendations and Suggestions from the Review of the European Stress Tests summarizes structure and focus of the Peer Review Process driven by ENSREG including Euratom Member States and the European Commission.

Based on the Stress Test report, ENSREG developed an Action Plan (AP) to track the implementation of the recommendations.

[17] WENRA Pilot Study on LTO, March 2011

[18] https://ec.europa.eu/energy/en/topics/nuclear-energy/nuclear-safety/stress-tests

[19] https://ec.europa.eu/energy/en/topics/nuclear-energy/nuclear-safety/stress-tests

[20] European Nuclear Safety Regulator's Group ENSREG, 1st Topical Peer Review "Ageing Management" Country specific findings, October 2018

[21] Convention on Nuclear Safety - CNS, Vienna Declaration on Nuclear Safety, 2015, IAEA INFCIRC-872

[22] Status Report of the Reactor Harmonisation Working Group (RHWG) Chair to WENRA, Fall 2018 Meeting, 25 October 2018

[23] Safety Requirements for Long Term Operation or Ageing Aspects and for Design, Construction and Operation of New Nuclear Power Plants, ENSREG Conference, Brussels, 29 June 2015, Dr. Hans Wanner, WENRA Chairman

ENSREG decided to prepare a consistent compilation[24] of peer review recommendations and suggestions, to assist the preparation or review of national action plans by national regulators, which was presented as European Level Recommendations with special emphasis on:

- European guidance on assessment of natural hazards and margins
- Containment integrity
- Prevention of accidents resulting from natural hazards and limiting their consequences

Other topics to be considered were:

- Topic 1 items (natural hazards)
- Topic 2 items (loss of safety systems)
- Topic 3 items (severe accident management)

The ENSREG compilation makes reference also to: WENRA Reference Levels, SAM Hardware Provisions, SAMG Validation, SAM Training, Level 2 Probabilistic Safety Assessments (PSAs), Severe Accident Studies including

- PSA analysis, including all plant states and external events for PSA levels 1 and 2.
- Radiological conditions on the site and associated provisions necessary to ensure MCR and ECR habitability as well as the feasibility of AM measures in severe accident conditions, multi-unit accidents, containment venting, etc.
- Core cooling modes prior to RPV failure and of re-criticality issues for partly damaged cores, with un-borated water supply.
- Phenomena associated with cavity flooding and related steam explosion risks.
- Engineered solutions regarding molten corium cooling and prevention of basement melt-through.

In the international nuclear safety frame, France joined the Convention on Nuclear Safety (CNS) under the auspices of IAEA as depository already at its initial phase in 1994. CNS creates as incentive convention safety obligations for land based nuclear power plants including soft verification instruments with a tri-annual peer review process. After the Fukushima Dai-ichi accident Contracting Parties requested a Diplomatic Conference to consider a possible amendment of the Convention and agreed by consensus on the adoption of the Vienna Declaration on Nuclear Safety (VDNS)[25].

Regarding existing NPP, the second principle of the Vienna Declaration re-quires: "*Comprehensive and systematic safety assessments are to be carried out periodically and regularly for existing installations throughout their lifetime in order to identify safety improvements that are oriented to meet the above objective. Reasonably practicable or achievable safety improvements are to be implemented in a timely manner*."

[24] Compilation of recommendations and suggestions Peer review of stress tests performed on European nuclear power plants, ENSREG 26 July 2012

[25] Convention on Nuclear Safety - CNS, Vienna Declaration on Nuclear Safety, 2015, IAEA INFCIRC-872

Also IAEA Safety Standards and Review Missions on generic and plant specific level providing guidance regarding strengthening safety at existing NPP together with LTO and ageing management, such as the IAEA Specific Safety Guide on *Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants*[26]

French nuclear safety experts are also involved in the ongoing drafting of an IAEA TECDOC on Experiences on implementing safety improvements at existing nuclear power plants based on the implementation of the VDNS principles.

This overview demonstrates key obligations established in European and international context of safety improvements for existing NPP, which have to be adequately and fully addressedby French nuclear safety regulations.

[26] IAEA SSG-48, Specific Safety Guide, Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants, 2018

2 RESULTS OF THE ANALYSIS OF THE MAIN SAFETY-RELATED TOPICS

2.1 Accident without core melt

Description of the facts (see also IRSN 2015a)

The design of Pressurised Water Reactors in the French Nuclear Power Plant Fleet France included originally only three levels of defence-in-depth.

After the accident at Three Mile Island Unit 2 in the United States in 1979, the concept of defence-in-depth was enlarged to include accidents that had not been explicitly considered during facility design. In particular, lessons from the initial probabilistic safety assessments and the TMI-2 accident demonstrated the need to take into account accidents resulting from multiple failures and those leading to core melt. These developments led to defining an additional level of defence-in-depth.

For reactors currently in operation, defence-in-depth is based on four levels intended to prevent the occurrence and limit the consequences of technical, human and organisational failures. The various levels of defence-in-depth apply in the various states of the facility, from normal operation to core melt accidents. At each level of defence-in-depth there are measures designed to prevent the occurrence of more severe situations.

Level 1: prevention of operating anomalies and system failures

Prevention of operating anomalies and failures in components, equipment and systems assumes prudent design (with adequate safety margins) and components, equipment and systems that have been manufactured and operated to the highest quality standards. This level corresponds to the normal domain of operation for the facility with general rules and operating procedures designed to maintain the plant unit within its normal operating domain.

Level 2: failure detection and comprehensive management of operating malfunctions

This level includes resources and systems designed to control operating malfunctions, which assumes monitoring that will ensure failures are detected. This includes automatic functions and control systems that can return the facility to its normal operating mode. These systems are designed to correct an abnormal change in facility parameters.

Level 3: ensuring basic safety functions during design-basis accidents

The first two levels of defence-in-depth reduce the risks of failure at the facility. It is nevertheless assumed that accidents can occur during reactor operation. Accidents considered at this level result from a single initiating event (e.g., the failure of a component essential for a basic safety function – comprehensive management of reactivity, cooling of nuclear fuel or containment of radioactive substances). Resources that limit the consequences of such accidents and en-

sure basic safety functions are implemented: at this level defence-in-depth consists of implementing safeguards that ensure the integrity of the core structure and limit releases into the environment in the event of an accident (considered for the design-basis of the facility). This level also includes defining emergency operating procedures.

Level 4: comprehensive management of severe accidents

This level of defence-in-depth includes procedures and equipment used to handle situations that are not covered by the first three levels of defence-in-depth; these are accidents that could result in reactor core melt. At level 4, the objective is to prevent accidents from resulting in core melt and to limit releases outside the site by ensuring containment of radioactive substances in the event core melt nevertheless does occur.

This level of defence-in-depth includes emergency procedures and associated equipment resources, specific equipment (e.g. hydrogen recombiners), the severe accident operating guidelines and the facility's on-site emergency plan. The licensee prepares and implements the on-site emergency plan. When the plan is implemented, the facility's emergency response teams are mobilised in order to contain the accident and avoid the release of radioactive substances. The purpose of the on-site emergency plan is to protect staff working at the site in the event of an incident or accident and to limit off-site consequences of an accident.

The thirty-four 900 MWe reactors in France are split into two main types:

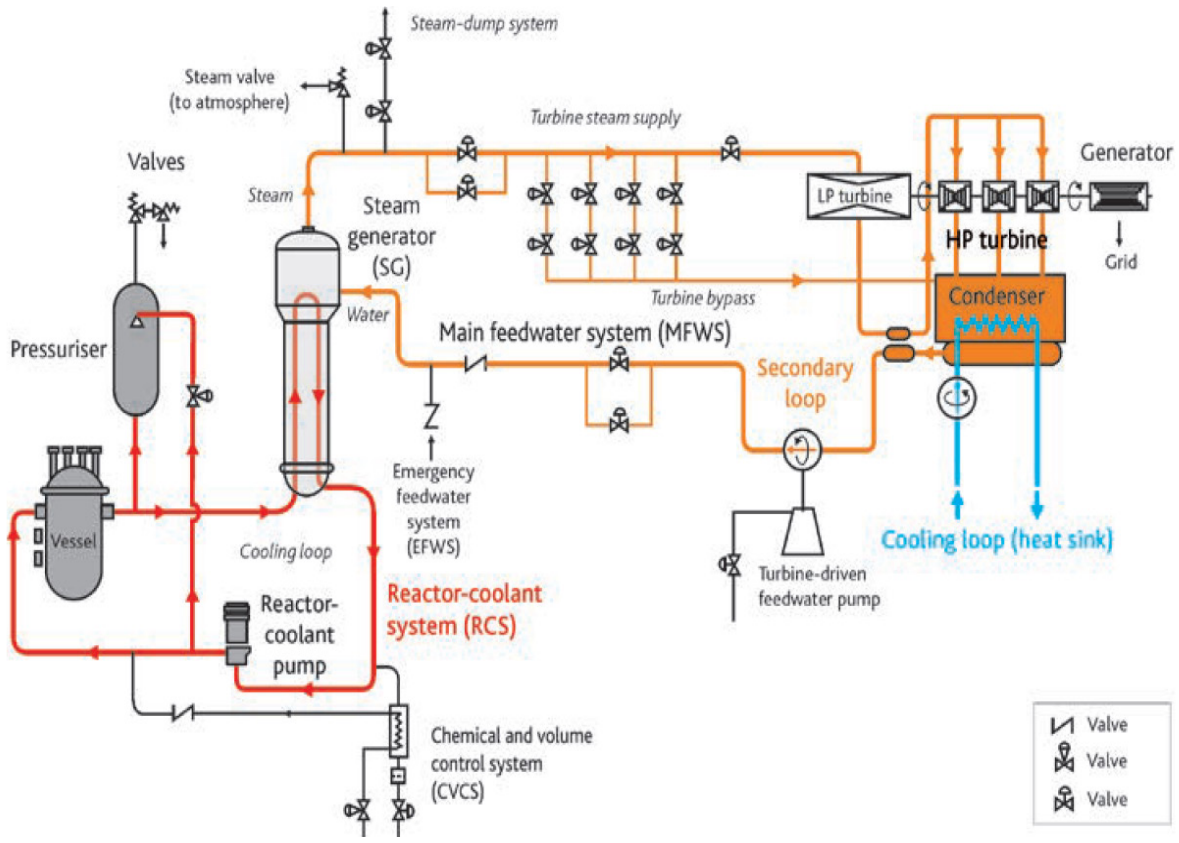
- CP0, which consists of the two reactors at Fessenheim and the four reactors at Bugey (the CP0 900 MWe series was brought into operation between 1977 and 1979);
- CPY (consisting of types CP1 and CP2), which encompasses the 28 other reactors (four reactors at Blayais, four at Dampierre, six at Gravelines, four at Tricastin, four at Chinon, four at Cruas-Meysse and two at Saint-Laurent-des-Eaux) (the CPY 900 MWe series was brought into operation between 1980 and 1987).

The CPY reactors benefited from the feedback obtained from the design studies, construction and operation of the CP0 reactors. Unlike the design studies for the CP0 series, which were conducted separately for each site, the design studies for the CPY series were conducted for all the sites. As a result, the CPY series differs from the CP0 series in terms of building design, siting of the engineered safety systems and more flexible reactor control (particularly via the use of control rods and the addition of control rods with less neutron-absorbing capacities). In the case of the CP2 reactors, the orientation of the control room was shifted by 90 degrees to prevent projectiles generated by rupture of the turbine generator from damaging the reactor containment vessel.

The reactor coolant system (RCS) carries heat away from the reactor core by circulating pressurised water through the three heat transport loops. Each loop is connected to the reactor vessel, which contains the core, and is equipped with a reactor coolant pump (RCP). This pump circulates the coolant heated through contact with the fuel elements to heat exchangers, called steam generators, where the coolant transfers its heat to the secondary loops and flows back to the reactor. The RCPs are fitted with seals that are continuously cooled

by pressurised water to prevent reactor coolant from leaking outside the RCS. The steam generators are evaporators composed of a bundle of U-tubes and a secondary side with integral moisture-separation equipment.

Schematic diagram of the main components of the RCS and the secondary loops



Source: IRSN (2015a)

umweltbundesamt

Figure 2: Schematic diagram of the main components of the RCS and the secondary loops.

The 900 MWe reactor containments consist of a single wall of prestressed reinforced concrete that is lined on the inside with steel plate (steel liner). The purpose of the steel liner is to act as a leaktight barrier, including during an accident. The purpose of the concrete containment is to withstand pressures and temperatures during an accident, seismic loads and external hazards.

The containments are fitted with a filtered venting system to prevent sudden containment failure in the event of a slow rise in the internal pressure during a core melt accident. To reduce the release of radioactive substances, the steam inside the containment is sent through this system to a system fitted a metal prefilter with a sand bed to trap most of the radioactive aerosols. This system is opened according to a specific procedure, known as U5. However, the filtered pressure relief devices are not qualified for the design basis earthquake.

The thickness of the basement also varies with each site. It is 1.5 m thick at Fessenheim, 2.25 m at Bugey, approx. 4 m for the CPY units.

The two main auxiliary systems are the chemical and volume control system (CVCS) and the residual heat removal system (RHRS). During normal operation, shutdown or restart of the reactor, the auxiliary systems contribute to fulfilling the basic safety functions (reactivity control, removal of heat from the RCS and of residual heat, containment of radioactive materials).

During reactor operation, the CVCS is used to adjust the boron concentration in the reactor coolant. The CVCS is also used to maintain the chemistry of the reactor coolant by adding chemicals (e.g., corrosion inhibitors) to reduce its concentration of corrosion products. It continuously supplies water to the seals of the RCPs to ensure their integrity.

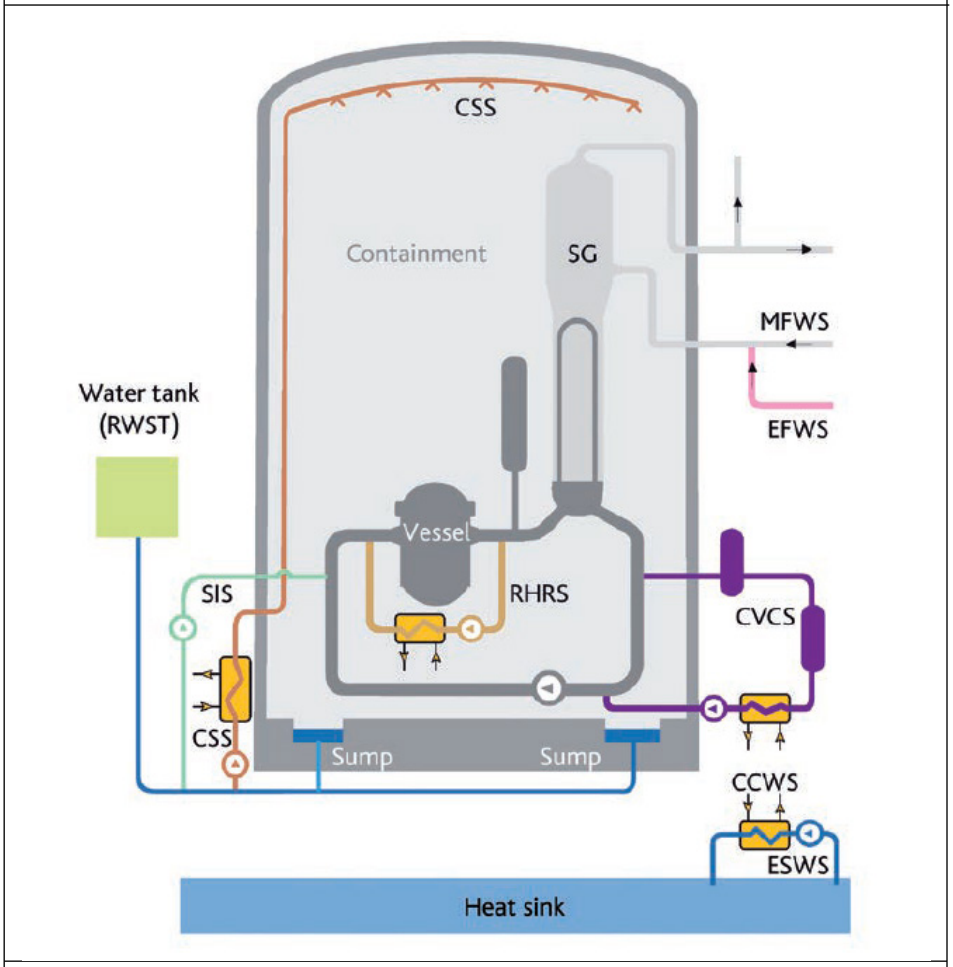
During normal reactor shutdown, the functions of the RHRS are to remove the residual heat generated by the fuel in the vessel. The RHRS, which has two motor-driven circulation pumps, collects water from a primary loop at the reactor outlet, transfers it to heat exchangers, and sends it back into another primary loop at the reactor inlet. The heat exchangers are cooled by the component cooling water system (CCWS), which is cooled by the essential service-water system (ESWS).

The engineered safety systems consist primarily of the safety injection system (SIS), the containment spray system (CSS) for the reactors in operation, and the steam generator emergency feedwater system (EFWS).

The SIS has pressurised accumulator tanks of borated water, a boric-acid tank (refuelling water storage tank, RWST) and pumps with discharge rates and pressures that can handle the various LOCA cases (breaks of different sizes). The reactors have a high-head safety-injection system and a low-head safety-injection system.

In the event of an accident leading to a significant increase in pressure in the reactor building, a water-spray system (CSS) is turned on to lower the pressure and thus preserve the integrity of the containment. In the case of the reactors currently in operation, the CSS, which is partially outside the containment, is used to spray water inside the reactor building. This water is pumped in from an external water tank (RWST) fed with sodium hydroxide, or from the bottom half of the containment (sump).

Schematic diagram of the main auxiliary systems and engineered safety systems



Source: IRSN (2015a)

umweltbundesamt

Figure 2: Schematic diagram of the main auxiliary systems and engineered safety systems.

The EFWS (emergency feedwater system) is used to maintain the level of water on the secondary side of the steam generators and thus cool the RCS in the event the main feedwater system (MFWS) is not available. It is also used during normal operation while the reactor is at hot shutdown to keep water in the steam generators.

The EFWS has two motor-driven pumps and either one pump is driven by a steam turbine supplied by the steam generators. These pumps draw in feedwater from a tank with a capacity of 700 m^3. However, the existing refill tank is not seismic qualified.

Other systems important to reactor safety include:

- the CCWS, which cools a number of items of equipment important to reactor safety (the RCPs and the CVCS pumps; the ventilation systems; the SIS and CSS). The CCWS operates in a closed loop between the auxiliary systems and the engineered safety systems on the one hand, and the ESWS on the other. It should be noted that the CCWS at the Fessenheim reactors does not contribute to cooling of the CVCS, the RCPs, the CSS or the ventilation systems. These systems and items of equipment are cooled directly by the ESWS;

- the ESWS, which cools the CCWS through the heat sink (river or sea). The 900 series have two ESWS trains;
- the fuel pool cooling and purification system (FPCPS), which, amongst other things, is used to remove decay heat generated by the fuel elements stored in the spent-fuel pool;
- the ventilation systems, which play an essential role in the containment of radioactive materials by placing rooms at negative pressure and filtering releases;
- the fire-protection circuits and systems;
- the instrumentation and control (I&C) system and the electrical systems. The systems important to reactor safety are powered by redundant power supplies consisting of two independent electrical trains. Each electrical train is supplied by a switchboard that itself is supplied by either the transmission grid (two independent high-voltage lines) or a diesel generator. In addition, a third diesel generator (GUS) may be used if necessary. For the 900 MWe series, this one ultimate backup diesel-generator set (GUS) per site is not qualified against earthquake. Nor is the GUS able to supply all safety equipment required at level of defence 3.

Systems used under reactor accident conditions

In accident situations without a break in the RCS, residual heat may be removed first by the EFWS, which is automatically initiated if the MFWS is not available.

In accident situations, a break in the RCS may be caused by a loop failure or the opening of the safety valves. For example, if a small break occurs on the RCS, the heat from the reactor core is not completely carried away by the coolant flowing out of the break and into the containment. A portion of this heat must be removed by the EFWS.

A sufficient water inventory is maintained in the RCS by the SIS, which pumps sufficient amounts of water into the RCS to compensate for breaks up to and including double-ended breach (complete rupture) of the RCS. This function is carried out for breaks of all sizes by two pumps that inject borated water at high pressure (trip threshold of 170 bar) and two pumps that inject borated water at low pressure (trip threshold: 10 bar). In addition, accumulator tanks containing borated water and pressurised with nitrogen empty their contents into the RCS if its pressure drops below 40 bar.

If an RCS break occurs, the CSS is actuated to lower the heat and pressure inside the containment. It does so by drawing in water from the RWST by means of two motor-driven pumps. When the RWST is empty, the CSS draws water from the sumps at the bottom of the containment. The water used by the CSS is cooled by the CCWS, which itself is cooled by the ESWS (at Fessenheim, this cooling is provided directly by the ESWS).

In some accidents with core melt that jeopardise the integrity of the containment, the heat inside the containment may be removed by the containment's filtered venting system. This system limits the peak pressure inside the containment (U5 procedure).

During normal operation and incident and accident transients, the facility is controlled according to a set of procedures whose purpose is to keep the reactor in a safe state or drive it into this state.

Supplementary procedures have been established for operating conditions involving simultaneous failure of the redundant trains of systems important to safety and for failure of equipment used over the long term (several months) after a loss-of-coolant accident (LOCA). Known as “H procedures” (“H” for *hors dimensionnement*, or, beyond design basis), these supplementary procedures may require the installation of new, supplementary equipment (e.g., addition of a turbine generator that produces electricity from the steam in the secondary loop to supply a power source for some essential systems, or the installation of a special generator. These procedures are as follows:

- procedure H1 for total loss of the heat sink or associated systems;
- procedure H2 for total loss of the steam generator feedwater supply (MFWS and EFWS);
- procedure H3 for total loss of the offsite and onsite power sources (loss of both offsite power sources, unsuccessful house-load operation, and loss of both generators);
- procedure H4 for total loss of the SIS or CSS over the long-term phase following a LOCA (future total loss of pumping or heat-exchange systems);
- procedure H5 for protection of some riverside sites against flooding above the thousand-year flood level.

In addition to the aforementioned accidents, there remains the possibility that a series of events could lead to radioactivity being released outside the facility. This is the case of core melt accidents. The following emergency procedures have been created to mitigate or delay core damage and radiological consequences:

- procedure U1 for averting core meltdown in situations where no H procedures would be suitable or effective. This procedure recommends, based on changes in the core outlet temperature and the availability of the systems and equipment, the best actions to be taken in terms of using the steam generators, SIS, and the relief valves on the pressuriser and the RCPs to prevent core meltdown;
- procedure U2 for locating and isolating containment leaks;
- procedure U3 for implementing mobile emergency equipment for the SIS and CSS and which supplements procedure H4;
- procedure U4 for implementing means of prevention of early radioactive releases in the event of vessel breach and corium erosion of the basement;
- the U5 procedure for relieving the pressure inside the containment *via* the sandbed filter.

In such a situation, the emergency-response teams use the Assistance Guide for Emergency-Response Teams (GAEC) and the Severe Accident Operating Guidelines (GIAG), which define the actions to be taken to ensure containment of radioactive substances for as long as possible.

Compilation of currently binding European and international safety requirements

According to the EU COUNCIL DIRECTIVE 2014/87/EURATOM of 8 July 2014 (EU 2014), the following nuclear safety objective for nuclear installations has to be applied,

"that nuclear installations are designed, sited, constructed, commissioned, operated and decommissioned with the objective of preventing accidents and, should an accident occur, 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 radioactive releases that would require protective measures that could not be limited in area or time."

This safety objective has to be achieved through a defence-in-depth concept[27]. *"This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant."* (EU 2014)

Based on (EU 2014), (WENRA 2014), and (IAEA 2016) have to be applied to ensure sufficient reliability of the equipment of level of defence 3 (safety equipment), the following **design principles**:

a) redundancy;

b) diversity;

c) segregation of redundant subsystems, unless this is conflicting with safety benefits;

d) physical separation of redundant subsystems;

e) safety-oriented system behaviour upon subsystem or plant component malfunctions;

f) preference of passive over active safety equipment;

g) the auxiliary and supply systems of the safety equipment shall be designed with such reliability that they ensure the required high availability of the equipment to be supplied;

h) automation (in the accident analysis, equipment that has to be actuated manually shall in principle not be credited until 30 minutes have passed).

[27] Paragraph 3.31 of the Fundamental Safety Principles (IAEA 2006) states that:
"Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available.... The independent effectiveness of the different levels of defence is a necessary element of defence in depth."

Independent layers of provisions

It shall be ensured by the defence-in-depth concept that a single technical failure or erroneous human action on one of the levels of defence 1 to 3 will not jeopardise the effectiveness of the measures and equipment on the next level.

Single-failure concept

The safety equipment necessary for the control of events on level of defence 3 shall be available redundantly and segregated in such a way that the safety functions necessary for controlling events are still sufficiently effective if it is postulated that, in the event of their required function,

- a single failure of a safety equipment with the most unfavourable effects occurs due to a random failure, and
- there is at the same time an unavailability of a safety equipment due to maintenance measures with the most unfavourable effects in combination with a single failure.

Common Cause Failures

Provisions to reduce the probability of occurrence of common-cause failures such failures shall be taken in such a way that a multiple failure of safety equipment on level of defence 3 need not be assumed. Redundant safety equipment for which possible common-cause failures have been identified, shall be installed in diverse manner as far as technically reasonable.

Internal hazards and external hazards

The design of the equipment shall be based on the following:

a) the respective most severe internal hazards or external hazards to be postulated;

b) the special characteristics of long-lasting external hazards;

c) combinations of several external hazards (e. g. earthquake, flood, storm, lightning) as well as of very rare human induced external hazards between them or combinations of these hazards with internal events (e. g. pipe break, internal fires, loss of offsite power); these combinations shall be postulated if the combined events may show a causal relationship or if their simultaneous occurrence has to be considered due to their probability and the extent of the damage caused.

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

- failures of pressure retaining components ;
- internal floodings;
- fires;
- internal explosions;
- internal missiles;
- load drops.

The external hazards to be postulated as having the most severe consequences shall be those that have to be postulated site-specifically according to the state of the art in science and technology. Here, the foreseeable future development of the site properties regarding the external hazards to be postulated shall also be taken into account.

Conservatism in the safety records

IRSN points out that safety must be demonstrated, taking into account by rules required conservatism (IRSN 2018)[28].

Accident Management

- Accident management shall comprise preventive and mitigative accident management measures as well as severe accident management guidelines for an emergency response staff to be formed in case of a severe accident.
- The equipment provided for internal accident management measures must impair neither normal specified operation nor the use of safety and emergency equipment as specified by their design. Their compatibility with the safety concept shall be ensured.
- The accident management measures rest on specially dedicated measures and equipment including equipment that is not permanently installed (mobile) as well as on the flexible use of available safety equipment, operating systems and emergency equipment.
- The measures and equipment provided for accident management shall remain effective even in the case of internal and external hazards as well as in the case of very rare human induced external hazards if these hazards may lead to multiple failures of safety equipment that is necessary in these situations and if these measures and equipment contribute to the mitigation of the effects of the respective hazards and very rare human induced external hazards.
- If spent fuel is stored in the spent fuel pool outside the containment, measures of the internal accident management shall be provided for the purpose of maintaining – by using all available measures and equipment – the integrity of the surrounding structural cover for as long as possible, excluding or limiting releases of radioactive materials into the environment, and achieving a long-term controllable plant state.
- The measures and equipment provided specially for accident management on level of defence 4 must not be used for demonstrating safety on the other levels of defence.

[28] *«Chaque réacteur fait l'objet d'une démonstration de sûreté s'appuyant, entres autres, sur un ensemble d'hypothèses sur les caractéristiques des composants de l'installation. Les hypothèses incluent des pénalisations (appelés « conservatismes ») pour couvrir les incertitudes sur les caractéristiques réelles (en regard des caractéristiques théoriques) des équipements (par exemple, le débit du système d'injection de sécurité dans le circuit primaire sera volontairement minoré dans certaines études de sûreté par rapport au débit requis pour ce système). Chaque composant doit donc rester conforme à des exigences permettant d'assoir la démonstration de sûreté (avec des marges).*

Si un équipement ou un matériau n'a pas la résistance ou les caractéristiques attendues (non-conformité), la démonstration de sûreté pourrait ne pas être acquise pour certaines situations. EDF devrait alors traiter cet écart. Si l'écart était important et si son traitement s'avérait impossible, cela pourrait conduire à l'arrêt de l'installation. » (IRSN 2018)

Diverse heat sink

Even in case of a loss of the primary heat sink as a result of loss of functions in the area of the circulating water intakes and returns, residual-heat removal from the plant shall be ensured under all operating states by a diverse heat sink (possibly also by different heat sinks in combination). The equipment needed for this purpose shall satisfy at least the requirements for internal accident management measures; their effectiveness shall be demonstrated. The availability of this diverse heat sink shall also be ensured in the event of external hazards.

List of reference transients, incidents and accidents[29] **(ASN 2014a)**

Reference transients, incidents and accidents within the plant have to be considered to demonstrate the safety of the plant**.**

- **Reference transients: Plant Conditions Category 2 (PCC 2)**
  - reactor trip (spurious),
  - feedwater system malfunction causing a reduction in feedwater temperature,
  - feedwater system malfunction causing an increase in feedwater flow,
  - excessive increase in secondary steam flow,
  - turbine trip,
  - inadvertent closure of one main steam isolation valve,
  - loss of condenser vacuum,
  - short term loss of offsite power (≤ 2 hours),
  - loss of normal feedwater flow (loss of all the main feedwater pumps and of the startup and shutdown pump),
  - loss of one reactor coolant pump without partial trip,
  - uncontrolled rod cluster control assembly bank withdrawal,
  - rod cluster control assembly misalignment up to rod drop, without limitation,
  - startup of an inactive reactor coolant loop at an incorrect temperature,
  - malfunction of the chemical and volume control system that results in a decrease in boron concentration in the reactor coolant,
  - malfunction of the chemical and volume control system causing an increase or decrease in the reactor coolant inventory,
  - primary side pressure transient (spurious pressurizer spraying, spurious pressurizer heating),
  - uncontrolled reactor coolant system level drop during mid-loop operation (state intermediate and cold shutdown),
  - loss of one cooling train of the residual heat removal during mid-loop operation (intermediate or cold shutdown).
- **Reference incidents: Plant Conditions Category 3 (PCC 3)**
  - small steam or feedwater system piping failure,
  - long term loss of offsite power (> 2 hours),

[29] In principle, only safety systems shall be used for the safety demonstration in order to reach and to maintain the safe shutdown state. (ASN 2014a)

- inadvertent opening of a pressurizer safety valve,
- inadvertent opening of a steam generator relief train or of a steam generator safety valve,
- small break loss of coolant accident,
- steam generator tube rupture (one tube),
- inadvertent closure of all the main steam isolation valves,
- inadvertent loading and operation of a fuel assembly in an improper position,
- forced decrease of the reactor coolant flow (all pumps),
- failures in liquid or gazeous waste systems,
- uncontrolled rod cluster control assembly bank withdrawal,
- uncontrolled single control rod withdrawal,
- rupture of a line carrying primary coolant outside of the containment (e.g. sampling line).

- **Reference accidents: Plant Conditions Category 4 (PCC 4)**
  - long term loss of offsite power (> 2 hours),
  - steam system pipe break,
  - feedwater system pipe break,
  - inadvertent opening of a steam generator relief or safety valve,
  - rod cluster control assembly ejection,
  - intermediate break and large break loss of coolant accident (up to the surge line break)
  - residual heat removal system break outside the containment,
  - reactor coolant pump seizure (locked rotor),
  - reactor coolant pump shaft break,
  - rupture of two steam generator tubes in one steam generator,
  - fuel handling accident,
  - boron dilution due to a non-isolable rupture of a heat exchanger tube.

Multiple failures conditions Risk Reduction Category A (RRC-A)[30][31] **(ASN 2014a)**

In addition to reference transients, incidents and accidents, multiple failures conditions have to be considered in the safety demonstration.

- **List of RRC-A**
  - station blackout: loss of offsite power cumulated with the failure of the two main diesel generators,

[30] Design Extension Conditions (without significant fuel degradation) (IAEA 2016)

[31] For the assessment of multiple failures conditions, all systems can be deemed available, except those which are assumed to have failed in the multiple failures combination. No additional failure and no unavailability due to maintenance have to be deterministically postulated in the systems needed to reach the final state. (ASN 2014a). These systems include in particular the "Hardened Safety Core".

- loss of the component cooling water system/essential service water system cooling chains,
- total loss of feedwater (loss of the main feedwater, emergency feedwater systems),
- small break loss of coolant accident and loss of the safety injection trains,
- small break loss of coolant accident and simultaneous loss of the component cooling water system/essential service water,
- anticipated transients without scram,
- rupture of several steam generator tubes (up to 10 tubes in one steam generator),
- steam line break and simultaneous steam generator tube rupture (up to one tube in the affected steam generator),
- steam generator tube rupture (one tube) with a main steam relief train stuck open at the affected steam generator,
- total loss of the spent fuel pool cooling system.

Compilation of deviations from the essential safety requirements

For the ASN and IRSN, the 900 MW reactors are expected to be in compliance with the safety requirements applicable to the EPR in the event of an extension of operation beyond 40a.(IRSN 2018)[32]

However, the IRSN also states that a number of EPR safety requirements cannot be met in the 900 MW reactors.(IRSN 2018)[33]

Basic deviations of the 900 MW reactors from the currently binding European and international safety requirements:

- All systems of the important secondary-side emergency feed system are based on a single reservoir, which means that they are meshed in their passive components (in some cases also via shared piping).
  The primary-side emergency cooling system, primary boron system, and fuel pool cooling system, also rely on a single reservoir, and these systems are also meshed with their passive components.
  Thus, no complete independence of these systems or their individual redundancies is given. If, for example, internal events such as a fire or a pipeline failure, or also due to external influences, result in a failure in these areas, the required safety functions would have been completely eliminated.

[32] *«Le renfort des exigences de sûreté des réacteurs concernés est un point essentiel pour garantir le meilleur niveau possible de protection des populations et des territoires vis-à-vis des risques d'accident. Le référentiel de sûreté défini pour le réacteur EPR a été considéré dès les premières instructions avec l'ASN et l'IRSN comme un objectif à viser en cas d'extension de la durée de fonctionnement des réacteurs actuels. Les leçons de l'accident de Fukushima ont ensuite conduit à compléter les exigences relatives aux agressions externes de très forte amplitude.»* (IRS 2018)

[33] *«À l'issue des quatrièmes visites décennales, des écarts vont subsister entre le niveau de sûreté de l'EPR et celui des réacteurs de 900 MWe post VD4, eu égard aux différences de conception significatives comme le nombre de trains de systèmes de sauvegarde, la disposition géométrique des enceintes de confinement et bâtiments adjacents (plus favorable à la récupération des fuites sur l'EPR), la cuve (absence de pénétration en fond de cuve sur l'EPR), la bunkerisation des piscines de désactivation du combustible, prévue à la conception sur le réacteur EPR mais non envisagée par EDF pour les réacteurs de 900 MWe.»* (IRS 2018)

- For feeding into the primary circuit with open reactor pressure vessel is a mobile feed pump (motopompe thermique mobile) ready at the site, which can feed coolant from the fuel pool in the primary circuit. It must not be more than one unit at the same time in a system state with open primary circuit according to the operating regulations. The mobile feed pump is not seismic qualified.
- There are no diversified systems or facilities for essential safety functions at safety level 3. Only in the area of the secondary-side steam generator feeding diversified driven feed pumps are available. However, their function depends on the availability of the steam generator, which is not guaranteed in a number of events.
- A number of safety-related components (safety level 3) are used for operational purposes (safety level 1).
- The safety systems are basically n + 1 of redundancy. However, for new systems (for example EPR), a higher degree of redundancy (n + 2) is required.
- A number of safety-related components are not seismically qualified. Thus, it can be assumed that these components are not available in the event of an earthquake.

The large number of deficiencies in the design of the safety systems of the 900 MW reactors significantly increase the risk of accident scenarios that may lead to core melt:

Accident scenarios that may lead to core melt[34]

- Loss-of-coolant accidents (LOCA): large breaks, intermediate breaks and small breaks

The accident scenarios that lead to core melt assume the failure of one or more engineered safety systems. Scenarios involving one of the following failures are considered for a reactor initially at power:

- failure of the SIS;
- failure of the CSS while in the injection and/or recirculation phase.
- Loss-of-coolant accidents with containment bypass (V-LOCA)
- Steam-line break accidents (SLB)
- Break in the feedwater line (FWLB)

The most likely accident scenarios where FWLB leads to core melt involve either (i) several control rods becoming stuck outside the core and preventing reactivity control or (ii) failed closure of the isolation valves on the lines of the steam generator affected by the break (thus preventing the secondary loops from cooling the reactor) followed by failure of maintaining a feed-and-bleed stream.

- Steam generator tube rupture accidents (SGTR)

[34] Severe accidents were not considered at the design stage of the generation II French PWRs. (IRSN 2015c)

SGTR (one tube or two tubes) accident scenarios that may lead to core melt include total loss of coolant from the secondary loop and failure of the SIS or implementation of feed and bleed by operators.

- Accidents with total loss of heat sink or associated systems

Core melt in a reactor at power may be caused by failure of the EFWS to supply the steam generators followed by failure to initiate feed and bleed or failure to maintain a sufficient amount of water in the RCS in the event of a break on the RCP seals.

- Accidents with total loss of the steam generator feedwater supply

The accident scenarios that may result in core melt include:

- failure of the TDAFWP (turbine-driven auxiliary feedwater pump) or injection of water to the RCP seals (which could lead to a break due to the loss of cooling) when the RCS is initially closed;
- failure of the RCS makeup when the RCS is open.
- Loss of onsite power (IRSN 2015b)

The accident scenarios that may lead to core melt therefore are primarily so called “TGTA-H2” scenarios (total loss of the steam generator feedwater supply and failure of feed and bleed) and scenarios that lead to breaks on the RCP seals and failure to maintain a sufficient amount of water in the RCS.

- Transients involving automatic shutdown failure (ATWS)[35]

These transients lead to loss of the MFWS and the EFWS is unable to remove the heat generated by the reactor core.

There may be three consequences:

- loss of integrity of the RCS when its design-basis pressure is exceeded;
- core damage (especially in the event of failure of cooling by the secondary side of the steam generators followed by failure of core cooling by feed and bleed);
- rupture of the steam generator tubes caused by the large difference in pressure between the primary and secondary loops.

Results of the EU Stresstest

As a result of the EU stress test, ASN has determined that, from its point of view, there is no need to immediately shut down one of the plants in operation (ASN 2012a). However, as a prerequisite for the continued operation of the facilities ASN calls for an immediate increase in the robustness of the facilities against extreme external events about the existing safety margins.

„Dans le même temps, l’ASN considère que la poursuite de leur exploitation nécessite d’augmenter dans les meilleurs délais, audelà des marges de sûreté dont elles disposent déjà, leur robustesse face à des situations extrêmes.“

[35] “Basically, ATWS events are considered as belonging to the beyond design basis accidents (BDBA) category” (IAEA 1999). Concerning /ASN 2014a/ ATWS belongs to the Risk Reduction Category A (RRC-A), and thus to level 3b of defense in depth concept (WENRA 2013).

In particular, a “noyau dur” (Hardened Safety Core, HSC) has to be installed to protect against beyond design external events, regardless of the question of the concrete probability of such event sequences (ASN 2017):

„L'apport de la démarche post-Fukushima et notamment la mise en place du noyau dur est de prévoir des dispositions permettant de faire face à des accidents initiateurs qui sont hors dimensionnement, éventuellement cumulés, indépendamment de leur probabilité d'occurrence. Cette démarche a pour objectif de couvrir les situations hautement improbables.”

With (ASN 2012a), ASN ordered the first measures or retrofits for the French plants in response to the results of the EU stress test (ASN 2011). Important measures to increase plant safety in response to the EU stress test continue to be outlined in the so-called National Action Plans (ASN 2012b, 2014b, 2017).

Essential retrofits are:

- technical facilities for the permanent removal of heat from the reactor and the fuel pool [ECS-1], [ECS-16],
- one additional ultimate diesel generator (Diesel d’ultime secours, DUS) per reactor, capable of supplying the Hardened Safety Core facilities with the required electrical energy, and a low-power emergency diesel generator (Mini-DUS), which is to be made temporarily available and is able to supply the control and lighting of the control room during a failure of the other electrical power supply [ECS-18],
- the establishment of a national rapid reaction force (Force d'Action Rapide du Nucléaire, FARN) [ECS-36] and
- the establishment of a local crisis staff building and the provision of additional mobile facilities.

According to (ASN 2012a) FARN must be able to reach every French plant site within 24 hours of the occurrence of an event and to provide the facilities there with mobile facilities and specially trained personnel. Furthermore, the construction of a “noyau dur” (Hardened Safety Core, HSC) has been requested by ASN for the French plants [ECS-1].

The facilities of the HSC should be independent of, and diversified from, existing facilities.

When designing the HSC, the external effects of earthquake, flooding, wind, lightning, hail and tornadoes shall be based on an increased impact strength compared to the original design.

HSC should have its own control equipment and its own electrical power supply, which is as independent as possible from the other facilities of the plant.

In addition, at all sites of the French nuclear power plants, a new local emergency centre building will be built to meet the requirements of the “Hardened Safety Core”. Construction work commenced at all sites in accordance with (ASN 2016).

The improvement of safety and the realization of the findings from the accident at the Fukushima nuclear power plant will take place in three phases (ASN 2017):

Phase 1 (2012-2015): deployment of temporary or mobile measures to enhance protection against the main situations of total loss of the heat sink ("H1 situations") or of the electrical power supplies ("H3 situations"):

- reinforcing the existing on-site emergency equipment (pumps, generator sets, hoses, etc.),
- installing medium-capacity ultimate backup diesel-generator sets,
- reinforcing the earthquake (SSE) resistance and flood resistance (maximum thousand year flood) of the emergency management premises,
- installing tappings for connecting mobile equipment, particularly the FARN's equipment,
- deployment of the FARN,
- implementing an automatic reactor trip in the event of an earthquake,
- installing electrically backed-up level measurement instrumentation in the pools.

Phase 2 (2015-2021): implementation of definitive design and organisational means that are robust to extreme hazards, notably the fundamental elements of the hardened safety core, designed to respond to the main situations of total loss of the heat sink or electrical power supplies beyond the baseline safety requirements in force:

- installation of a large-capacity ultimate backup diesel-generator set, including the construction of a dedicated building before 31 December 2018,
- setting up of a dedicated ultimate water source,
- setting up of an ultimate water makeup source for each reactor (on the PTR reactor cavity and spent fuel pit cooling and treatment system and the steam generators emergency feed water supply systems) and each pool,
- reinforcing the earthquake resistance of the containment venting filter, installation of sodium tetraborate baskets to reduce the emission of gaseous iodine in a severe accident situation on reactors that do not have SIC (silver-indium-cadmium alloy) control rod clusters,
- installation of the first protections against extreme flooding (high-intensity rainfall and earthquake-induced rupture of tanks) in addition to the existing protected volume measures,
- implementation of means for detecting reactor vessel melt-through or the presence of hydrogen in the containment,
- installation of the first devices which, in the event of a break in the transfer tube or the pool compartment drainage pipes, prevent exposure of the fuel assemblies during handling and enable them to be placed in a safe position using the emergency manual controls,
- reinforcing the operating teams so that they are capable of managing all the extreme situations studied in the stress tests,
- construction on each site of an emergency centre capable of withstanding extreme external hazards (functionally independent in an emergency situation).

Phase 3 (as of 2019 on the occasion of the periodic safety reviews): this phase supplements phase 2, in particular to improve the level of coverage of the potential accident scenarios considered. EDF indicates that these means have also been defined with a view to continuing operation of the reactors beyond forty years:

- removal of the residual heat by the steam generators by means of an independent ultimate backup feed water system supplied by the ultimate heat sink,
- addition of a new makeup pump on the primary reactor coolant system,
- finalisation of the ultimate makeup connections, through fixed systems, to the steam generator auxiliary feed water supply system, to the PTR tank and to the spent fuel pool,
- installation of an ultimate instrumentation & control system and the definitive instrumentation of the hardened safety core,
- installation of a reactor containment ultimate cooling system (that does not require opening of the containment venting-filtration system),
- implementation of a solution for flooding the reactor pit to prevent corium melt-through of the basement.

Meanwhile, a decision by ASN is in place that provides for the postponement of a large-capacity ultimate backup diesel generator set, including the construction of a dedicated building on December 31, 2020. (IRSN 2016). For the NPP Fessenheim the installation is no longer necessary, since Fessenheim is to be shut down in the period from 2020 to 2022.

In this context, ASN (ASN 2017) again points out that the requirements of the ASN are to be considered as part of the continuous process with which the safety of the existing facilities is linked to the state of safety of the reactors Generation III:

„De façon générale, les demandes de l'ASN s'inscrivent dans un processus d'amélioration continu de la sûreté au regard des objectifs fixés pour les réacteurs de troisième génération, et visent, en complément, à faire face à des situations très audelà des situations habituellement retenues pour ce type d'installation."

EDF itself sees the implementation of Phase 3 measures as a long-term project until about 2030 (FERRARO 2015, p. 9).

Results

- ASN[36] and IRSN[37] assume that the safety level of the 900 MW reactors will not reach the safety level of the EPR even after extensive retrofitting. (IRSN 2018), (OECD 2015)[38]
- For IRSN and ASN, a lifetime extension is more of a problem because a number of components are only designed for 40a (IRSN 2018[39]; IRSN 2018a, ASN 2018)[40], (OECD 2015)[41].

[36] Autorité de sûreté nucléaire

[37] Institut de Radioprotection et de Sûreté Nucléaire

[38] France actually expresses expectations for its reactors to reach an improved safety level during LTO that is ideally similar to new Generation III NPPs. (OECD 2015)

- Removal of existing deviations in the 900 MW reactors from basic safety requirements of safety level 3 safety systems (e.g., increasing redundancy, independence of safety systems) is not provided by the present documentation for an extension of the service life. Retrofitting in the safety systems is concerned with improving the reliability of existing systems and will essentially take place between 2019 and 2030. IRSN (IRSN 2018)[42] and ASN urge a quick elimination of existing deviations. (ASN 2018)[43]
- Bunkering of spent fuel storage facilities, as required for the EPR, is not planned in the project to extend service life [44].
- The large number of deficiencies in the design of the safety systems of the 900 MW reactors significantly increase the risk of accident scenarios that may lead to core melt.
- There is currently no publicly available documentation for the analysis of the reference transients (PPC 2), incidents (PPC 3) and accidents (PPC 4) and multiple failures conditions (RRC A).
- However, the supervisory authority refers to the planned retrofitting in connection with the "Hardened Safety Core" (HSC). However, the HSC is classified as a 4th level safety system. In addition, the 4th level of safety is required as an additional and independent level compared to the level 3 safety level.

---

[39] *«L'extension de la durée de fonctionnement au-delà de 40 ans présente un caractère particulier car certains composants des réacteurs français (circuits primaires notamment) ont été conçus en retenant, dans les études de dimensionnement, une hypothèse de fonctionnement pendant 40 ans. Pour ces composants, de nouvelles études démontrant leur aptitude au fonctionnement sur une durée supérieure à 40 ans sont donc nécessaires.»* (IRS 2018)

[40] *«Par ailleurs, la maîtrise du vieillissement et de l'obsolescence et le maintien de la qualification des matériels représentent un enjeu important du quatrième réexamen périodique des réacteurs de 900 MWe puisque certains matériels seront amenés à fonctionner au-delà de leurs hypothèses initiales de conception.»* (ASN 2018)

[41] *"At the design stage, systems, structures and components (SSCs) were designed under the cumulative loading and environmental conditions for an assumed 40 years of operation."* (OECD 2015)

[42] *«Phase 3 (de 2019 à 2033) : à la fin de cette phase, l'ensemble des moyens déployés sur les installations permettra de couvrir, avec des équipements fixes, les situations les plus extrêmes considérées dans le cadre des Études complémentaires de sûreté (ECS). Ces équipements (nouveaux ou existants renforcés) permettront notamment le refroidissement des réacteurs par le circuit secondaire (générateur de vapeur) ou une gestion améliorée des accidents graves (évacuation de la puissance hors de l'enceinte de confinement sans recourir au dispositif d'éventage-filtration, stabilisation du corium par étalement et renoyage sur le radier). Ces moyens permettront également de répondre aux objectifs de sûreté définis pour l'extension de la durée d'exploitation des réacteurs. EDF prévoit de déployer ces moyens à l'occasion des visites décennales des réacteurs, soit pour les différents paliers :*

- *réacteurs à eau pressurisée de 900 MWe : 2019 à 2030 (quatrième visite décennale) ;*
- *réacteurs à eau pressurisée de 1300 MWe : 2025 à 2032 (quatrième visite décennale) ;*
- *réacteurs à eau pressurisée de 1450 MWe : 2029 à 2032 (troisième visite décennale).»* (IRSN 2018), (ASN 2017), (IRSN 2016)

[43] *«L'ASN vous a également demandé de corriger au plus tard lors de la quatrième visite décennale de chaque réacteur de 900 MWe les écarts ayant un impact sur la sûreté qui auront été préalablement identifiés. Les écarts détectés au cours de ladite visite décennale devront être corrigés dès que possible, en tenant compte de leur importance pour la sûreté.»* (ASN 2018)

[44] *«Une bunkerisation n'est pas prévue par EDF dans son projet d'extension de la durée de fonctionnement de ces derniers.»* (IRS 2018)

Therefore, facilities of the 4th level of safety cannot be used to compensate for existing deficits on the third level of safety mentioned here.

- The protection of the planned HSC against extreme external events is in accordance with the requirements for new installations. In contrast, the protection of existing facilities remains practically unchanged.

2.2 Internal/external hazards

2.2.1 Description of the facts

External hazards have a potential for simultaneous impairment of effectiveness of all levels of safety of the defence-in-depth concept of a nuclear power plant. A robust protection concept against external hazards is therefore of particular importance for the safety of nuclear power plants.

External hazards shall be taken into account in the design of the plant. In addition to natural hazards[45], human made external hazards shall be taken into account in the design of the plant according to site specific conditions. Corresponding requirements are specified in the Safety Standards of the IAEA in (IAEA 2006, Requirement 17), a list of requirements concerning external hazards to be considered in the design of nuclear power plants, i.a. earthquake, flooding, plane crash, contains (IAEA 2016)[46]. Especially with regard to the design against natural hazards, it is required in (IAEA 2006) that cliff-edge effects have to be excluded [47].

The concept of “cliff edge effects” appears in the IAEA Safety Standards in the Safety Requirements for Nuclear Power Plant Design /1/ when it is required that the safety analysis using the probabilistic approach shall provide confidence

[45] WENRA Rev.- Level T2,2
Natural hazards shall include:
- Geological hazards;
- Seismotectonic hazards;
- Meteorological hazards;
- Hydrological hazards;
- Biological phenomena;
- Forest fire.

[46] In (IAEA 2016), the essential requirements for earthquakes are listed under 3.1-3.4, for flooding under 3.18-3.32 and for aircraft crashes under 3.44-3.47.

[47] 5.21. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects. (IAEA 2006)

that small deviations in plant parameters that could give rise to severely abnormal plant behaviour will be prevented.[48]

Basic requirements for the consideration of external hazards with regard to the assessment of the safety of nuclear power plants are specified by the IAEA in (IAEA 2006, 2016) and WENRA in (WENRA 2014, 2015). In accordance with the recommendations of the IAEA, WENRA requires in the Ref. Level E5.2 the consideration of external hazards in the design of nuclear power plants.

According to WENRA Ref. Level F2.2 (WENRA 2014), beyond design external hazards shall also be considered. In Ref. Level F3.1 is required that even under such conditions cliff-edge [49]effects must be excluded.

In France, general requirements apply with regard to the consideration of external hazards in terms of the safety of NPP (ORDER 2012, Article 3.6).

Nevertheless, deficits regarding the design against "extreme" natural hazards are found:

"Regarding the robustness against natural hazards, safety equipment needed for design basis accidents are generally protected against design basis hazards, which is in particular the case for safety equipment required in case of a LOOP (e.g. diesel generators). Simultaneous occurrence of an external hazard with a multiple failures situation, such as the total loss of all electrical sources, was not systematically postulated."

However, according to "defence-in-depth" and recognizing that both LOOP (Loss Of Off-site Power) and LUHS (Loss of the Ultimate Heat Sink) of long duration are likely to be induced by some natural hazards, some equipment used to manage these situations are protected against some hazards. Equipment required in severe accidents are generally not designed to resist to natural hazards as it is considered that such hazards could not lead to core damage."(IRSN 2015a)

Also in the context of the operating experience is reported on a deficient design against natural hazards in the operating nuclear power plant (ASN 2018):

- Seismic
  - Seismic resistance fault in the Donzère-Mondragon canal embankment which protects the Tricastin NPP
  - Significant safety event rated level 2 on the INES scale concerning a seismic resistance flaw on the auxiliary systems of the backup diesel generating sets[50]

[48] Potential for causing cliff edge effects – Both analyses and experience data show that some external hazards would cause cliff edge effects and others result in incremental increase of damage. Seismic loads are good examples of the latter while flooding would be an example of an external event with the potential to cause cliff edge effects. The behaviour of safety related SSCs at the Fukushima Daiichi NPP clearly underlined this difference. The IAEA Fukushima Fact Finding Mission Report provides the information that in the 45 minutes between the seismic actions being felt at the plant and the arrival of the destructive tsunami waves, the fundamental safety functions of the six units were very likely in place even though.

[49] the seismic loads exceeded the calculated hazard values significantly. For external hazards that have a high potential for leading to cliff edge effects, it may be necessary to use larger safety margins. (SMIRT 2015)

- Significant safety event concerning a lack of seismic resistance of the surge tanks of the emergency diesel generators cooling systems
- Internal flood
  - Leaktightness flaw in the penetrations necessary for managing an internal flood[51]
  - Significant safety even rated level 2 on the INES scale concerning a risk of total or partial loss of the heatsink for 29 reactors

2.2.2 Natural hazards

2.2.2.1 General facts

The basic requirements for the consideration of natural hazards regarding the safety of nuclear power plants are described in the Specific Safety Guides SSG-9 (IAEA 2010a) (earthquake) as well as for flooding in SSG-18 (IAEA 2010b).

In IAEA SSG-18 (IAEA 2010b) are pointed out in 2.18 possible climatic changes in the site of the nuclear plant, which can have an impact on safety.[52.]

In the WENRA Ref. Level T4.2 (WENRA 2014) is specifically required that nuclear power plant against impacts like earthquakes or flooding with an exceedance probability of 10^{-4}/a have to be designed.[53]

Where it is not possible to calculate these probabilities with an acceptable degree of certainty, an event shall be chosen and justified to reach an equivalent level of safety.

The general approach to seismic hazard evaluation should be directed towards reducing the uncertainties at various stages of the evaluation process in order to obtain reliable results driven by data. The overall uncertainty will involve both aleatory uncertainties, and epistemic uncertainties (IAEA 2010a)

---

[50] https://www.usinenouvelle.com/article/le-nouveau-rate-d-edf-dans-le-nucleaire-concerne-cette-fois-les-diesels-de-secours-post-fukushima.N819840

[51] Internal flooding leading to electrical equipment downtime:
EDF has implemented measures at its facilities to guard against the risk of internal flooding. These are aimed in particular at precluding the risk of simultaneous flooding of both redundant electrical trains in reactor safety-related systems. However, two recent events at the Fessenheim and Le Blayais plants, where water flowed through openings that were not watertight, highlighted certain weaknesses in nuclear reactor electrical rooms regarding the risks of internal flooding. (IRSN 2014a)

[52] 2.18. Climatic variability and climate change may have effects on the occurrence of extreme meteorological and hydrological conditions. Over the lifetime of an installation, it is possible that the climate at the site will undergo significant changes. (IAEA 2010b)

[53] T4.2 The exceedance frequencies of design basis events shall be low enough to ensure a high degree of protection with respect to natural hazards. A common target value of frequency, not higher than 10^{-4}per annum, shall be used for each design basis event. Where it is not possible to calculate these probabilities with an acceptable degree of certainty, an event shall be chosen and justified to reach an equivalent level of safety. For the specific case of seismic loading, as a minimum, a horizontal peak ground acceleration value of 0.1g (where 'g' is the acceleration due to gravity) shall be applied, even if its exceedance frequency would be below the common target value. (WENRA 2014)

The WENRA Ref. Level T4.3 (WENRA 2014) also requires a comparison with historical events: *"The design basis events shall be compared to relevant historical data to verify that historical extreme events are enveloped by the design basis with a sufficient margin."*

All measures and equipment required to perform the basic ("fundamental") safety functions must be designed against external hazards.

According to WENRA Ref.-Level E8.3 (WENRA 2014) only systems that are suitably safety classified can be credited (WENRA Safety Issue G) to carry out a safety function.

With regard to non-classified systems, it must be ensured that these systems do not cause negative effects (WENRA Ref.-Level T5.4[54](WENRA 2014).

According to WENRA Ref-Level T6.1 (WENRA 2014) is required that events that are more severe than the design basis events shall be identified as part of DEC analysis.

2.2.2.2 Earthquake

With regard to the design against earthquakes, according to WENRA Ref. Level T4.2 (WENRA 2014) is required: "The exceedance frequencies of design basis events shall be low enough to ensure a high degree of protection with respect to natural hazards. A common target value of frequency, not higher than 10^{-4} per annum, shall be used for each design basis event".

In France in relation to the requirements for the protection of nuclear power plants against the earthquake impacts currently are to be used the requirements of the fundamental safety rule n ° 2001-01 (ASN 2001).

According to this, the French protection concept for protection against earthquakes is based on the so-called "Maximum Historically Probable Earthquakes" (Séismes Maximaux Historiquement Vraisemblables – SMHV) considered to be the most penalising earthquakes liable to occur over a period comparable to the historical period, or about 1000 years." (ASN 2001**,** BERGE 2014)[55].

Based on this, a so-called "Safe Shutdown Earthquakes" (Séismes Majorés de Sécurité – SMS[56]) (ASN 2001) is determined.

A simple equation with reference to the site-based earthquake intensity I will be applied:

$$I\,(SMS) = I\,(SMHV) + 1$$ [57]

[54] For each design basis natural event, the necessary SSCs should be identified and classified in accordance with Issue G, taking due consideration of the credible combination of the event with other events, and qualified against the event under consideration or protected by suitable measures. The performance of non-safety SSCs should also be considered to avoid potential secondary damage to necessary SSCs. (WENRA 2015)

[55] However, according to /ASN 2017, 3.3.3.2.7/ for natural impacts, an exceedance probability of 10^{-4} per year should apply, but a deterministic approach applies to impacts from earthquakes (ASN 2017, 3.3.3.2.9)

[56] *"Definition of a "Safe Shutdown Earthquakes" (SMS) to account for uncertainty on the definition of MPHE, which may be completed by paleoseismological evidences." (*IAEA 2012)

The seismic level determined by (ASN 2001) at the minimum is 0.1g[58],[59] (BERGE 2016).

It is assumed that the safe shutdown earthquake SMS of the 900 MW systems has an exceedance probability of 10^{-4} per year (IRSN 2014).

With regard to the design of the "Hardened Safety Cores", increased requirements apply in France60. The design requirements for the "Hardened Safety Core" are listed in (CNS 2014, IRSN 2015a) [61],[62]. With the assignment of the

[57] "A one-degree increase in intensity corresponds to an increase in magnitude conventionally set at 0.5." (IAEA 2012)

[58] "The spectrum adopted by the licensee for sizing its installation may not be less than a minimum fixed spectrum with acceleration at 0.1 g and infinite frequency." (IAEA 2012)

[59] see also (ASN 2017)

[60] "In this context of 'Hard Core' definition, the Safety authority asked all the operators to propose, for each NPP, a 'Hard Core seismic Level' 'significantly higher than seismic level currently defined in the regulation'.

The current regulation to assess the seismic hazard for NPP is presented in the first section of present article, and is the deterministic RFS 2001-01.

Then, in 2013, operators proposed their Hard Core seismic levels mainly based on a flat rate increase of the Safe Shut Down Level (combined with paleo event if any), homogeneous on the whole frequency band. These Hard Core Levels are still under instruction by the IRSN, technical support of the ASN, which recently asked the operators to complete their justifications by performing probabilistic seismic hazard assessments (PSHA) to associated return periods to the Hard Core Seismic Levels. The requirement is that this return period should be 'significantly higher than the 10^{-4} return period currently being the reference for NPP design', conforming the ENSREG recommendation resulting from the European Peer review". (ASN 2012)

[61] „The design requirements for HSC are detailed in:

The components of the "hardened safety core" are considered as important to safety and assigned to the so called "IPS-NC" classification, which corresponds to the third level in the international safety classification system (IAEA Guide referenced DS367).

The hardened safety core have to be :

- composed of a limited number of Systems, Structures and Components (reliability),
- protected against extreme earthquake, flood and tornado, explosion, lightning, extreme climatic conditions, wind, snow, accidental rain, hail storm, wind generated missiles...
- protected against the effects that could be induced by these hazards,
- operable even if all other components are out of service (e.g. dedicated electrical source and I&C),
- operable without any material or human support from the outside during 24 hours following the event until FARN set-up (Nuclear Rapid Intervention Force),

All the Hardened Safety Core SSCs have a specific Safe Shutdown Earthquake called SND. The SND is 1.5 times higher than the SSE of the other safety systems of the plant. Note that the SND is defined with the respect of the SSE based on the site seismology. The 1.5 factor is of the order of magnitude of the margins between the Maximum Historically Probable Earthquake (MHPE) and the SSE."(CNS 2014)

[62] *"Main SSCs of the HSC and their support (such as electrical distribution and switchgears for example) should be as far as possible:*

- *independent from the existing SSCs, to ensure that the HSC constitutes the expected ultimate line of defense and isn't affected by the potential failures that may occur on the other parts of the installation,*
- *diversified from the existing SSCs to limit the risks of common cause failures, notwithstanding the objective of sufficient reliability of new equipment"* (IRSN 2015a)

"Hardened Safety Core" to the so-called "IPS-NC" this System in France has been classified as a safety-related system (ASN 2015).

According to available information, the "Hardened Safety Core" against earthquakes is as follows designed: *"All the Hardened Safety Core SSCs have a specific Safe Shutdown Earthquake called SND. The SND is 1.5 times higher than the SSE of the other safety systems of the plant. Note that the SND is defined with the respect of the SSE based on the site seismology. The 1.5 factor is of the order of magnitude of the margins between the Maximum Historically Probable Earthquake (MHPE) and the SSE."*(CNS 2014)[63]

According to (EUR 2012) applies for the design against earthquakes:

„For new NPPs, the level of the beyond design basis earthquake ground motion to be considered is established through applicant requirements (for instance, the U.S. Utilities Requirements Document (URD), and the European Utilities Requirements Document (EUR) (EUR 2012), and through regulatory requirements."

In the USA, new NPPs are being licensed through the "Certified Design" process. These NPP's Certified Designs are designed to broad-banded ground response spectra anchored to 0.3g peak ground acceleration (PGA) (considering three directions of input motion) and a broad range of site conditions. The design basis ground motions are termed the Certified Seismic Design Response Spectra (CSDRS). These CSDRS are compatible with the specifications of the URD. The Certified Design is performed for a wide range of generic site conditions intended to envelope 80% of the U.S. potential sites for new NPPs.

The USA practice for design certification is to perform a PRA (Probabilistic Risk Analyses)-based SMA (seismic margin assessment) to determine a lower bound on plant capacity referred to as a plant-level "high confidence of low probability of failure" (HCLPF). In this process, the PRA methodology utilizing event trees and fault trees is applied, but the resulting plant conditional probability of failure is not convolved with a hazard to obtain the CDF. For the US Certified Designs, a plant HCLPF capacity of at least 1.67 times the DBE (design basis earthquake) (CSDRS) is required to be demonstrated.

The European Utility Requirements document (EUR) has specified similar requirements for standard designs in Europe, i.e. DBEs comprised of broad-banded ground response spectra anchored to a PGA of 0.25g and consideration of beyond design basis earthquake events in the design phase. The EUR specifies that it should be demonstrated that a standard design achieves a plant seismic margin of 1.4 times the DBE.

(The new) Regulatory requirements in France follow the EUR: they require the demonstration of a plant HCLPF capacity of 1.4 times the DBE on a site specific

[63] In addition french side (EUROSAFE 2016) supplement:

"Licensees must define a HSC reference seismic spectrum meeting the following requirements:

- Be 50% higher than the seismic spectrum chosen as a reference for the design of new nuclear facilities
- Be conservative of spectra defined accordingly to a probabilistic manner with a return period of 20 000 years (PSHA)
- Take into account the possible effects due to the facility location including the nature of the soil"

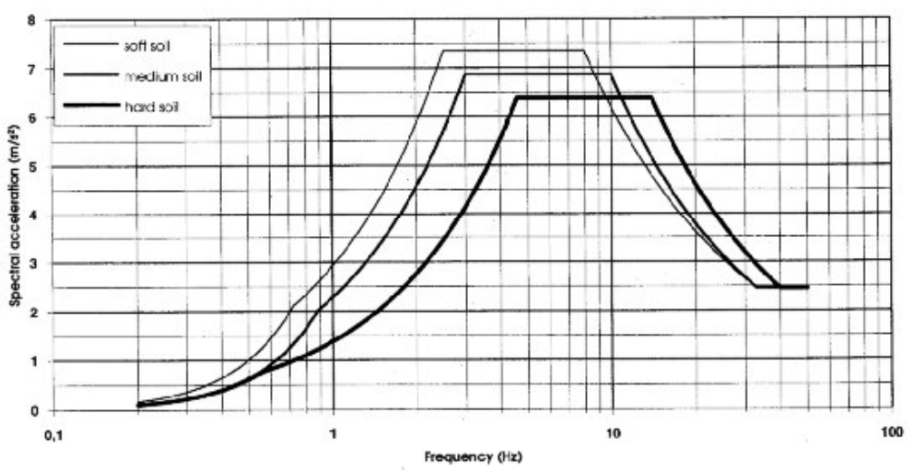
basis, preferably using deterministic methods. Generally, worldwide, countries have adopted the BDB earthquake philosophy of demonstrating margin of 1.67 or 1.4 times the DBE."

The requirements of the EPR (ASN 2014a) allow two possibilities regarding the design of the nuclear power plant against earthquakes:

- Site-specific spectra and acceleration values (Fig. 1) or
- Standardized design against intensity VIII earthquakes on the MSK scale

Figure 3: Earthquake spectra for the design of the EPR.

Earthquake spectra for the design of the EPR



Source: ANS (2014a)

umweltbundesamt

2.2.2.3 External flooding

In the WENRA Ref. Level T4.2 (WENRA 2014) is required that nuclear power plant against impacts such as earthquakes or flooding with an exceedance probability of 10^{-4} per year shall be designed.

In France is used to protect against flooding the ASN Guide GUIDE N° 13 in the Version 08/01/2013 (ASN 2013).[64]

Regarding flooding of nuclear power plant sites in the area of rivers is defined as reference in (ASN 2013): *"The reference flow rate corresponds to the peak flow rate associated with the thousand-year return period flood, taking the upper bound of the 70% confidence interval, and increased by 15%."*[65]

[64] The flooding risk was reassessed following the Blayais flooding in 1999. Following the partial flooding of the Le Blayais nuclear power plant in December 1999, the licensee updated its safety margin level (CMS) evaluation of all the sites and systematically took account of other hazards liable to cause flooding.

[65] *"The reference level is the maximum level on the site resulting from the reference flow rate. In some particular site configurations, a higher water level can be reached with a lower flow rate than the reference flow rate; in such cases the reference level is the level corresponding to this lower flow rate."* (ASN 2013)

The requirements for the design of French systems against flooding were previously specified by the RFS 1.2.e of 1984. According to this, flooding conditions and the failure of barrages are to be taken into account as possibilities for a flooding of the plant at river locations.

A maximum flood (Cote Majorée de Sécurité, CMS) is defined by RFS 1.2.e as being the highest water level resulting from the 1,000 year flood with a statistical reliability of 70%, with a safety margin of 15% on the discharge rate so determined (Crue fluviale, CF) or from the failure of an upstream barrage in superposition with a centenary flood (Rupture de Barrage, REB).

In response to the flooding event at the Blayais site in 1999, additional events were introduced These include contributions from high winds on river flood levels (Influence du Vent, IVF), an increase in the groundwater level (Remontée de la Nappe Phréatique, NP), a failure of dykes or pipelines (Dégradation d'un Ouvrage de Canalisation, DOC), heavy rain and continuous rain events (Pluies de Forte Intensité, PFI sowie Pluies Régulières et Continues, PRC), a failure of water-bearing components in the unit (Rupture de Circuits et d'Equipements, RCE) and occurrence of tidal waves (Intumescence, INT). Furthermore, seismic flooding scenarios are to be considered.

To take into account the influence of strong winds IVF, the wave height is superimposed on a 1,000-year flood (70% confidence interval) due to strong winds with a centenary wind speed (70% confidence interval). The possible increase in the groundwater level NP is being tested site-specifically, especially under the conditions of the flood event CMS. For the rain events, the heavy rainfall PFI is based on the 95% confidence interval for the centenary rainfall, which is to be overlaid with an average water level of the river. The continuous rainfall PRC is the 24-hour averaged rainfall of a centenary rainfall, which is to be overlaid with a one-hundred-year high water level.

2.2.2.4 Other natural external hazards

EDF (EDF 2011) considers earthquakes and external flooding as well as other external influences from the outside wind (direct impacts and projectiles), hail and lightning.

The procedure for determining the reference level for river locations in (CNS 2014, Question No.180) was explained in more detail

"The flood safety level is the higher of the two following levels:

- *Level reached by a river whose flow is obtained by increasing the thousand year flood level by 15%*
- *Level reached by the combination of:*
  - *the flood wave resulting from the most penalizing upstream dam failure event,*
  - *and the 100-year river flood (or the highest historical flooding event if this is higher)"*

"In the guide of ASN relative to the flooding hazards, that has been published in 2013, even if it's not explicitly mentioned, the set of reference flood situations (RFS) to take account for the design have been defined using a common probabilistic target to have a certain homogeneity between all the RFS. In compliance with the international practices, the RFSs should have a probability of exceedance of 10^{-4} per year, in order of magnitude, and should cover associated uncertainties."(CNS 2014)

Thus, in the context of preparatory work for the third periodic safety review, an investigation into potential damage from projectiles in high winds was carried out. As a result, it was found that intake manifolds of the emergency feed pump outside buildings, the air cooling of emergency diesel, other pipelines of emergency diesel, the connecting lines and fittings between the reservoirs ASG and SER and other safety-related components could be affected by projectiles.

ASN (ASN 2017b) notes that the operator has provided studies on other external environmental impacts: in-depth analyzes on the effects of snow loads, wind loads, hail and lightning. In particular, safety-relevant components that are installed outside of buildings are to be investigated.

According to ASN (ASN 2016), EDF concludes that projectiles triggered by strong winds cannot affect buildings containing safety-related components. Wind speeds of up to 200 km/h were investigated, which is supposed to correspond to an exceedance frequency of approx. 10^{-4} per year.

According to ASN (ASN 2014b), the assumptions underlying the other external factors vary more frequently in their frequency than those of earthquakes or floods.

According to ASN (ASN 2016), EDF, with regard to the required protection against lightning, is based on the level of protection specified at the time of the original design of the installations against a lightning effect with an exceedance probability of 10^{-2} per year per reactor. Analyzes of the operator would show a high degree of robustness compared to the underlying lightning effects, a cliff-edge effect was not to be feared. With regard to the requirements for the HSC, however, higher requirements with regard to lightning protection would be required. According to (FERRARO 2015), these requirements mean a maximum lightning current of 300 kA.

According to ASN (ASN 2016), effects of snowfall related to flood risks were discussed but not classified as relevant. A protection of the buildings against snow loads was ensured according to the rule revised in the year 2000. According to (ASN 2017c) snow loads are taken into account according to Eurocodes specifications.

2.2.2.5 Results (natural hazards)

- Several technical anomalies detected by EDF exist on various equipments in French NPP. Most of these anomalies are related to a lack of resistance to earthquake and exist since the construction of the plants" (ANS 2017a)[66] Affected are a variety of pipelines, the diesel generators, safety-related auxiliary systems, fire protection equipment.
- In terms of external events, the state of the art and technology for the design must be based on events that, with due regard for uncertainties, have an exceedance probability of less than 10^{-4} per year. The determination of the magnitude of these effects shall be carried out using deterministic and, as far

[66] "Several technical anomalies detected by EDF on various equipments
Diesel generators auxiliary systems
Fire fighting pipes
Most of these anomalies are related to a lack of resistance to earthquake and exist since the construction of the plants" (ANS 2017a)

as possible, probabilistic methods according to the state of the art and technology. If such events cannot be determined with sufficient reliability, deterministic design events must be determined instead, which ensure comparable safety.

- The previous design of the systems against external hazards in various areas is based on requirements according to the conventional regulations. Since the conventional regulations require a much lower level of safety than is required for nuclear facilities, it is unlikely that this would result in an interpretation equivalent to a level required today in France and internationally at an exceedance probability of 10^{-4} per year, taking into account all uncertainties. The exceedance probability of the deterministic SMHV is on the order of 10^{-3} per year, for the SMS the intensity is set by one intensity level higher than for the SMHV. According to ASN, an increase in intensity by one on the MSK scale basically means a doubling of the acceleration parameters. Therefore, this generally leads to a probability the derived design event in the order of 10^{-4} per year.
  The per annum exceedance probabilities of seismic actions at the site as well as the uncertainties of these values shall be determined using the probabilistic seismic hazard analysis. Such analyses are not available for all sites of the 900 MW plants.
- Basis for the deterministic determination of the design basis earthquake must be the strongest earthquakes that have occurred. Paleoseismic findings[67] shall be taken into account.
  The deterministic approach to specifying the design basis earthquake shall be based on historic earthquakes, taking the earthquake with the largest seismic actions into consideration that would have to be assumed at the site in light of current scientific knowledge.
  The design basis earthquake is described by the seismic actions at the location of the site that are characterized, essentially, by the intensity and ground motions. The design basis earthquake shall be determined and specified based on deterministic and probabilistic analyses.
- The extent to which the required probability of exceedance is actually guaranteed, taking into account all uncertainties, has not been proven without a site-specific probabilistic seismic hazard analysis. Such probabilistic seismic hazard analyzes are now state of the art in science and technology. It has also been shown in international analyzes that such specific risk assumptions can be substantial, in part by factors 2-3, above the originally deterministic assumptions.
- A number of safety-related components are not qualified seismically. Thus, it can be assumed that these components are not available in the event of an earthquake. Specific to the emergency power supply is that the previously installed as a reserve diversified emergency power supply is not seismic qualified and therefore cannot be credited even as a rmargin in an SMS. It is also not designed for additional rare external impacts such as a plane crash.

[67] Paleoseismology is a method used to search for indications of prehistoric quakes in geological sediments and rock formations and includes estimation of their magnitude and of the age of the deformations due to earthquakes. Paleoseismology serves to extend earthquake findings into the younger geological times.

- Further reservoirs existing on the plant site, which could be used to supplement the secondary coolant supplies of the emergency feed system, are not seismically qualified, so that even under the conditions of the safety earthquake on which the design is based, it cannot be assumed that these reserves will be available.
- In particular, for the reservoir of the emergency feed system and the flood reservoir low reserves are reported, which could possibly still be under a factor of 1.5. The ASN notes that the previously reported reserves are insufficiently resilient. The operator also credits reserves which are introduced as part of the design to hedge existing uncertainties. In case of failure of the flood reservoir PTR, central safety functions to control an earthquake are no longer available.
- ASN notes that the protection of safety equipment against earthquake-triggered fires must be improved as essential fire safety measures are not designed to address the effects of the SMS.
- According to (ANS 2014b), the measures for the mitigation of severe accidents installed in existing plants are not designed to withstand external impacts. While the installed passive autocatalytic recombiners (PARs) are designed for the removal of hydrogen from design basis accidents against the effects of earthquakes, this does not apply to PAR for the removal of hydrogen from beyond design basis accidents as well as for the filter systems of the filtered pressure relief.
- There are measures to increase earthquake resistance. It is not known whether this will eliminate all existing deficits.
- The facilities of the “Hardened Safety Core” are intended to achieve a significant increase in robustness against earthquake-induced impacts. First of all, according to the timetables for the establishment of the "Hardened Safety Core", a substantial increase in robustness compared to the previous external influences on which the design is based will only be achieved with the implementation of the extended facilities of the “Hardened Safety Core” from about 2020 becomes.
- The stability of buildings in the case of beyond design earthquakes is problematic. In the event of such an earthquake, accessibility to the temporary measures and facilities of Accident Management cannot be guaranteed. Thus, their accessibility is not ensured under such circumstances.
- The three main safety functions (reactor shut down, heat removal, confinement of radioactivity) have to be assured in the case of a flooding at the CMS level. As a consequence of the Le Blayais event, an increased flooding level has been defined for each site. The facilities of the "Hardened Safety Core" are to be based on a maximum flood as being the highest water level resulting from the 1.000 year flood with a statistical reliability of 70%, with a safety margin of 30% on the discharge rate so determined. In contrast, the protection of existing facilities remains practically unchanged.

2.2.2.6 Civilization-induced impacts

In accordance with WENRA Ref. Level E5.2 (WENRA 2014), the safety of the installation must also be guaranteed against civilization-induced impacts in addition to the natural hazards.

Among the civilization-related impacts include the accidental plane crash (hereinafter referred to as plane crash).

In the WENRA ref. Level F4.7 (WENRA 2014) it is further required that the residual heat removal from the reactor core and the fuel pool also in the case of beyond external impacts must be possible. Specific load assumptions in relation on the plane crash in the WENRA Ref. level are not explicitly stated.

According to (FLAB 1984, EDF 2011, U.S. Reg. 1984) French nuclear power plants should be by structural protection against impacts from the crash of smaller aircraft (Cessna 210 or Lear Jet 23), a military fighter aircraft of the type Phantom IV or an airliner protected.

The different load-time functions are in (FANC 2015) explained.

According to (FLAB 1984, ASN 1980) the French nuclear power plants were designed, based on probabilistic analyses, against the impacts from small civil aircraft («les petits avions civils (aviation générale, de masse inférieure à 5,7 tonnes) »)[68].

In (FLAB 1984) is carried out for this purpose: *„These statistical studies lead to the conclusion that, as far as the structures of standard 1 300 MWe plants are concerned, the only risk to be provided for in France is that resulting from the crash of a general aviation aircraft. Two types of general aviation aircraft are taken into account in the design of these buildings:*

- *A 'hard' projectile (with mainly perforating action): engine (0.2 t) of single-engined CESSNA 210 (1.5 t at 360 km/h);*
- *A 'soft' projectile (causing mainly shock of impact): twin-engined LEAR JET (5.7 t at 360 km/h).”*

The current requirements in France for the design of the EPR against plane crashes are indicated in (ASN 2014a).

The different approaches to design against aircraft crash in the existing France NPPs can be represented as follows:

“The RFS (RFS-I.2.a. du 05/08/1980) (ASN 1980) requires an assessment of the frequency of damage to the three main safety functions, for two types of airplanes (Cessna 210 and Learjet 23) of the general aircraft traffic. Protection is considered as acceptable if the frequency is lower than a determined value, which is a probabilistic objective.

[68] *«Concernant les chutes d'avions, les règles fondamentales de sûreté (RFS) applicables distinguent, pour la construction des installations nucléaires, 3 familles d'avions :*

- *les petits avions civils (aviation générale, de masse inférieure à 5,7 tonnes) ;*
- *l'aviation militaire ;*
- *l'aviation commerciale (avions de masse supérieure à 5,7 tonnes).*

Compte tenu des probabilités de chute de ces avions sur les installations nucléaires, celles-ci sont construites depuis les années 70 pour résister sans dommages à l'impact de la chute d'avions de la 1ère famille, les petits avions civils. Elles ne sont pas construites pour résister sans dommages à l'impact d'autres avions, dont les probabilités de chute accidentelle sont extrêmement faibles. En la matière, les règles françaises ne diffèrent pas de la pratique internationale. » (FLAB 1984, ASN 2001a)

The Technical Guidelines (ASN 2014a) require a deterministic approach, based on load-time diagrams C1 and C2 representing the crash of a military airplane. The Reactor Building, the Fuel Building and some auxiliary buildings[69] shall be designed against these load cases."

The recently published ASN Guide de l'ASN n ° 22 (ASN 2017) has not be further clarified of load characteristic in the event of a plane crash in relation to RFS-I.2.a. du 05/08/1980 (ASN 1980), a reference to (ASN 2014a) is not made.

In accordance with the requirements in France (ORDER 2012, Article 3.10), safety analyzes have to be updated whenever there are indications of changes of probabilities of external hazards. A component in periodic safety reviews is a reassessment of hazard-related risks (ASN 2016a), including the evaluation of the plane crash situation. Regulations for continuous safety improvement of nuclear power plants in France are indicated in (ORDER 2012, Chapter VII).

2.2.2.7 Results (civilization-induced impacts)

- However, on the basis of the information available, no recent assessments could be found on the basis of the available information for the hazard analyzes based on the original design of the french nuclear plants due to aircraft crashes, which could have led to a reassessment of the threat to the site due to a possible change in the probability of occurrence of a plane crash.
- If a larger aircraft crashes on a 900 MW system, failure of all important safety functions cannot be ruled out. Thus, the danger of core melt scenarios is given here.
- Backfitting measures to eliminate the existing deficits are not known.

[69] see concrete illustrations in /EdF 2011/

3 CORE MELT ACCIDENTS

3.1.1 Description of the facts

The design of the French 900 MWe reactors didn't take Severe accidents (SA) into account. However, as a result of previous PSRs, equipment and measures for the SA management (e.g., Passive Autocatalytic Hydrogen Recombiners (PARs), Emergency Filtered Containment Venting System (EFCVS)) were im-plemented. However, the EU stress tests revealed a number of shortcomings that need to be remedied during the forth PSR. Further improvements are en-visaged to meet the ASN´s objectives for the life time extension.

3.1.1.1 Results of the EU Stress tests

The EU stress tests revealed that the protection of the severe accident equipment against external hazards (earthquake, especially) was not considered before the Fukushima Daichi accident. Recommendation specific to France resulting from the ENSREG peer review in 2012: Several equipment items required for severe accident management are not qualified for earthquakes […]. The passive autocatalytic recombiners designed for withstanding design-basis accidents are qualified to seismic standards whereas those designed to withstand severe accidents are not […]. The hydrogen recombiners and venting filters currently used on the reactor fleet will have to be qualified for external hazards. (ASN 2017)

Regarding severe accident management (SAM), the stress tests in 2011 pointed to the following deficits of the 900 MW reactors:

- The Probabilistic Safety Analysis (PSA) does not include earthquake or any accident associated with the spent fuel pool.
- Only one emergency diesel generator is available per site, but it is not designed to withstand an earthquake.
- Fire detection and fixed extinguishing systems are not electrically backed-up by seismically qualified equipment.
- Current organisation and studies do not sufficiently address the management of a multi-unit accident.
- Habitability and accessibility of the emergency management rooms and control rooms in the case of filtered venting is not guaranteed.
- Instrumentation dedicated to SAM, able to detect reactor vessel melt-through and the presence of hydrogen in the containment is missing.
- Filtered venting systems are not seismically qualified. Also, the filters do not retain iodine, which is responsible for short-term exposure of people living in the NPP vicinity.
- The severe accident management guidelines (SAMGs) do not cover accidents in the spent fuel pool (SFP), and do not include multi-unit events.
- There is no bunkered emergency control room.

National Action Plan

Measures to remedy these deficits are described in the National Action Plan (ASN 2012). The progress of these actions was updated in 2014 and 2017. On the basis of the opinions of the Advisory Committee and the conclusions of the European stress tests, ASN issued a series of resolutions dated 26th June 2012 requiring EDF to implement (ASN 2017):

- a "hardened safety core" of material and organizational measures which, in the event of an extreme external hazard, are designed to ensure:
- a local emergency centre allowing emergency management of the nuclear site as a whole in the event of an extreme external hazard;
- a Nuclear Rapid Intervention Force (FARN) which, using mobile means external to the site, can intervene on a nuclear site;
- a range of corrective measures or improvements, notably the acquisition of additional communication and radiological protection means, the implementation of additional instrumentation, extensive consideration of internal and external hazard risks, improvement of the way in which emergency situations are taken into account.

ASN stated: To take account of the engineering constraints involved in these major works but also the need to introduce the necessary post-Fukushima improvements as soon as possible, their implementation is planned in three phases (see chapter 4m).

Phase 2 should be completed in 2021. Measures of particular importance for SAM are:

- reinforcing the earthquake resistance of the containment venting filter,
- implementation of means for detecting reactor vessel melt-through or the presence of hydrogen in the containment,
- reinforcing the operating teams,
- construction of an emergency centre on each site.

Phase 3 (as of 2019 on the occasion of the periodic safety reviews) supplements phase 2, in particular to improve the level of coverage of the potential accident scenarios considered. EDF indicates that these means have also been defined with a view to continuing operation of the reactors beyond forty years.

Measures of particular importance for SAM are:

- Finalization of the ultimate makeup connections, through fixed systems,
- Installation of an ultimate instrumentation & control system and the definitive instrumentation of the hardened safety core,
- Installation of a reactor containment ultimate cooling system (that does not require opening of the containment venting-filtration system),
- Implementation of a solution for flooding the reactor pit to prevent corium melt-through of the basemat.

The implementation of the "hardened safety core" and the provisions of phases 2 and 3 in particular, require validation of the design hypotheses for the material provisions and verification that the solutions proposed by EDF can meet the safety objectives set and that they are technologically achievable. On the basis of the files transmitted by EDF and the studies carried out, ASN asked its Advisory Committee for Reactors (GPR) to submit its opinion on the more important points of these files. Three meetings of the GPR have been held in 2016/2017. (ASN 2017).

On the basis of this review, ASN asked EDF for clarifications and additional studies. (ASN 2017). For 2019, four GPR review meetings to examine the files to be transmitted by EDF to clarify the design of the systems and their implementation procedures are envisaged (1. Severe accidents, 2. Demonstration of accident coverage, 3. Ability to manage complex accident situations including the sufficiency and robustness of the fixed and mobile equipment, 4. summary of stress tests).

Progress of the activities to remedy shortcomings of the SAM

In this section only some measures are discussed, the others are mentioned in the next sections.

Hydrogen monitoring system

The installation of redundant instrumentation dedicated to severe accident management, able to detect reactor vessel melt-through and the presence of hydrogen in the containment was speeded up to ensure that the reactors are equipped with redundant measurement instrumentation before 31/12/2017.

Reliable depressurization of the reactor coolant system

A hardware modification to improve pressuriser safety relief valve opening reliability, decided before the Fukushima accident and already applied on certain reactors, is planned for the fourth 10-year outage of each reactor.

Geotechnical containment

ASN has instructed EDF to examine the feasibility of installing technical devices such as a geotechnical containment or a system with an equivalent effect to prevent the transfer of radioactive contamination to groundwater in the event of a severe accident leading to corium melt-through of the reactor vessel. EDF has concluded that a geotechnical system at economically acceptable costs is not feasible. ASN has examined this file jointly with other provisions currently being studied to avoid basemat melt through, ASN nevertheless insists that EDF continues its studies on this subject. All these additional measures will be examined by the advisory committee in 2018 - 2019.

Filtered venting

EDF has submitted a detailed study of the possible improvements to the U5 venting-filtration system, considering in particular its resistance to hazards. EDF is going to proceed with seismic reinforcement of the U5 venting-filtration system. (ASN 2017) However, the existing filter system will be reinforced only to withstand the MHPE (maximum historically probable earthquake). This is not in compliance with WENRA requirements (see chapter 2)

The presently installed venting system is able to trap aerosol fission products, but it is not efficient to trap gaseous fission products such as molecular or organic iodine or noble gas. But according to EDF, in case of a core melt accident, silver released from the control rods and deposited into the sumps water would enable iodine stabilization in the sumps.

However, according to IRSN the gaseous iodine releases coming from the upper part of the containment would not be fully affected by the iodine stabilization in the reactor building sumps and have to be considered. Furthermore, there is

still an interest to examine the possibility to upgrade the existing EFCVS to reduce the gaseous iodine releases. According to IRSN (2017), this topic will be discussed during the next steps of the safety review process.

Habitability of the control room

EDF has planned reinforcing the electrical backup of the control room ventilation-filtration by the ultimate backup diesel generator set (DUS). Pending installation of the DUS, a modification is in progress to allow the resupply of one train of the ventilation system (DVC/DCC) of the control room by a medium-capacity ultimate backup diesel generator set, the "GE LLS".

Presence of hydrogen in unexpected places

In an accident situation, hydrogen can be produced inside the reactor vessel during the core degradation phase due to the oxidation of fuel element cladding and other materials present in the reactor vessel, or outside the vessel during the corium-concrete interaction, and by radiolysis of the water in the spent fuel pool. The hydrogen can also come from damaged hydrogen transport lines. On completion of the stress tests, EDF undertook to study the hydrogen explosion risk in the other peripheral buildings of the reactor containment. According to IRSN (2019), errors were found in the models produced by EDF. Therefore, the studies on the consequences of a leak of hydrogen in the nuclear island are not sufficient yet. (IRSN 2019)

Support to the personnel on site

EDF has reinforced the current emergency organisation, particularly by setting up a Nuclear Rapid Intervention Force ("FARN") with material and human resources. The FARN is a national-scale organisation, which will be capable of rapidly providing material and human aid to one or more sites in difficulty simultaneously.

The FARN comprises a national headquarter and four regional centres situated on the Bugey, Civaux, Dampierre and Paluel NPP sites. The regional centres have on-call intervention pillars of 14 people. The equipment is stored in premises specific to each centre. The FARN has transport and handling equipment, redundant telecommunication means and equipment for ensuring the resupply of water and electricity (pumps, compressors, diesel generator sets, etc.). (ASN 2017)

3.1.1.2 Objectives of Fourth ten-yearly outage of 900 MWe reactors

This chapter discusses the aims of the forth ten-yearly outage of the 900 MWe reactors in particular concerning the severe accident management.

In September 2010, EDF presented the programme of guidelines concerning the extension of the operating life of the reactors beyond forty years (operating life used as the design basis for certain structures and equipment). In June 2013, on the basis of IRSN´s review, ASN defined the objectives for the fourth PSR: improvement of facility safety to attain a safety level similar to that specified for the third generation nuclear reactor under construction at Flamanville (EPR). This requires changes to limit the radiological impacts of accidents without core melt, to prevent or mitigate the impacts of accidents with core melt (severe accidents) and to reinforce the safety of stored spent fuel.

To meet these objectives, EDF presented the guidelines for the fourth PSR of the 900 MW reactors in late 2013. EDF proposed among other suggestions the following severe accidents objectives: Review of the conditions of reactor operation and severe accident management with the aim of reducing the risks of early or large radiological discharges and the radiological consequences of accidents (excluding severe accidents) to tend towards situations where it is not necessary to deploy population protection measures.

Analysis of the 2013 guidelines for the periodic review associated with the 900 MW fourth ten-yearly reactor safety reviews.

IRSN reviewed the guidelines presented by EDF and presented its assessment to the Advisory Committee for Reactors in early April 2015. IRSN considered that the guidelines of the periodic review associated with the fourth ten-yearly reactor safety reviews were ambitious and unprecedented in size: they cover around fifty technical topics and aim at a safety substantial improvement. . IRSN also noted that some points needed improvment (IRSN 2016).

Following an analysis of the various elements supplied by EDF, and after asking the opinions of IRSN and the Advisory Committees of Experts for nuclear reactors in 2015, ASN issued a position statement on EDF guidelines for the fourth periodic safety review of the 900 MWe reactors on April 20 2016. In this document ASN asked EDF to introduce several additions to the envisaged programmes for oversight and analysis. These demands include in particular an evaluation of the impact of integrating the requirements applicable to installations presenting more recent objectives and safety practices.

After examination of the programme proposed by EDF, ASN stated that the topics selected by EDF are of relevance to the safety issues. However, ASN requested EDF to supplement several aspects of its programme,

- Improved management of accidents with core melt, more specifically with analysis of the steps aiming to reduce the frequency and consequences of core melt situations with opening of the containment venting filtration system:
- Demonstration of the qualification of the equipment necessary in the event of an accident with core melt.

According to ASN (2018a), ASN asked EDF to define the safety objectives to be used for VD4-900 review under those applicable to the new generation of reactors, including the EPR-FA3 reactor.

Fulfillment Report

The recently published Fulfillment report describedthe objectives for the VD4-900 PSR and the measure to meet these objectives.(EDF 2018).

Regarding core-melt accidents the Fulfillment Report stated that, for the fourth periodic safety review, EDF is seeking to ensure that the likelihood of early and large releases remains extremely small (around 10-7/year*reactor), whilst taking measures to avoid long-term environmental consequences. (EDF 2018a)

EDF's ambition is therefore to improve safety in the event of core meltdown accidents with regard to the EPR-FLA3 safety objectives, the mitigation measures taken at the design stage which make it possible to apply measures to protect populations and are very limited in space and time.

In order to achieve this goal, EDF is seeking to ensure that the following measures can be taken in the event of a core-melt accident:

- Residual heat can be removed from the core without opening the containment pressure relief system (known as U5);
- in degraded conditions with the consequential formation of corium, which melts through the reactor vessel, the corium can be stabilized on the reactor building base-mat, there-by remaining contained.

In order to achieve these objectives, EDF will take the following measures on top of the existing measures:

- Installation of a new "hardened core" containment-cooling system for cooling the corium either inside or outside the reactor vessel and for removing residual heat without having to use the containment pressure relief and gaseous release filtration system;
- the capture of any leaks from this "hardened-core" containment-cooling system in order to more effectively stop contamination from spreading in the event of a core-melt accident;
- stabilisation of corium once the latter has spread across the reactor-building base-mat and has been flooded with water, thereby guarding against the potential loss of containment due to base-mat melt-through;
- enhanced seismic resistance of the containment pressure relief and gaseous release filtration system.

3.1.1.3 Safety measures agreed or realized for the reduction of potential radioactive releases in the framework of PLE

The reactors of the 900 MW series were not designed to withstand a core melt accident. The Plant Life Extension (PLE) program, in order to give a possibility to extend lifetime beyond 40 years, includes some reinforcements toward closing the gap in the safety objectives of new reactors such as the EPR. Several safety reinforcements for severe accident are or are being implemented:

- Development and update of severe accident management guidelines (SAMGs);
- Installation of an Emergency Filtered Containment Venting System (EFCVS);
- Installation of Passive Autocatalytic Recombiners (PARs);
- Reinforcement of the closure system of material access penetration for the 900 MWe PWRs reactor building (above the design pressure);
- Instrumentation to detect hydrogen in the reactor containment and vessel failure;
- Modification of the pressurizer safety valves (reliability in case of station black out);
- Reinforcement of electrical supply of the containment isolation system and optimization of procedures for the manual actions;

The PLE program has been reviewed since 2010 by IRSN for ASN.

IRSN (2017a) stated: *"Even if all these reinforcements bring very substantial risk reduction, especially for the short term of any severe accident, it has to be recognized that there are some important gaps with the solutions developed for a Gen III reactor like EPR."* For example, in severe accident situations, it is diffi-

cult to demonstrate that the corium can be stabilized after vessel failure. Another important limit is the protection of severe accident equipment against external hazards. That means that the efficiency of the long-term accident management strategies for the Gen II PWRs is still limited in comparison with the efficiency of the EPR strategies.

Safety objects associated to the reduction of potential radioactive releases in the framework of PLE

As mentioned above, ASN requires that the safety objectives of the Gen III reactors (e.g. EPR) should be used as a reference for all studies undertaken in the frame of PLE. For EPR, the general objective is *"to achieve a significant reduction of potential radioactive releases due to all conceivable accidents, including core melt accidents"*. It means:

1. For accident situations without core melt, there shall be no necessity of protective measures for people living in the vicinity of the damaged plant (no evacuation, no sheltering);
2. Accident situations with core melt which would lead to large or early releases have to be "practically eliminated": if they cannot be considered as physically impossible, design provisions have to be taken to design them out. This objective applies notably to high pressure core melt sequences;
3. Low pressure core melt sequences have to be dealt with so that the associated maximum conceivable releases would necessitate only very limited protective measures in area and in time for the public. This would be expressed by no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in consumption of food.

The first objective is mainly related to Steam Generator Tube Rupture (SGTR) and Loss of Coolant Accident (LOCA) design basis accidents. The fulfillment of the first objective is discussed in chapter 2 of this expert statement.

The second objective has been largely addressed by the modifications which have been summarized above. However, there are remaining issues associated to uncertainties in the studies, which are relevant for both the second and the third objectives: effects of an ex-vessel steam explosion, effects of an uncontrolled injection of non-borated water during accident progression, risk for hydrogen and increase the in-vessel corium stabilization possibility. (IRSN 2017a, b)

To meet the third objectives, two remaining issues have to be considered to extend the design conditions (DEC):

- The long-term stabilization of the corium in case of vessel failure which cannot be demonstrated for all conditions
- The containment filtered venting system (EFCVS) decontamination factor (for gaseous iodine) which is not sufficient to limit need for emergency protective measures of population at the immediate vicinity of the plant.

Low pressure core melt accidents

Some IRSN statements after a first-step review of the EDF upgraded severe accident mitigation strategies for the 900 MWe reactors to meet the third safety objective, is discussed in the following chapter. (IRSN 2017a, b)

To meet the above mentioned third objective, EDF has included two upgrades in its PLE program:

1. A strategy to allow corium stabilization without concrete basemat melt-through
2. A strategy to remove heat from the containment without venting

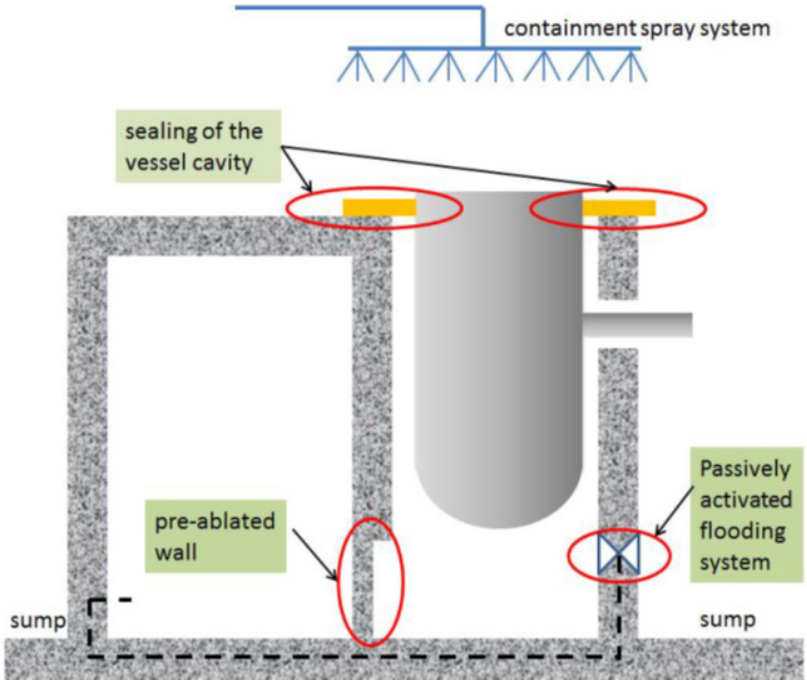
Modification to avoid concrete basemat melt-through

To limit the risk of reactor basemat melt-through by molten core after RPV failure, EDF has planned the following strategies:

- The vessel cavity (reactor pit) is modified to avoid any water entry before vessel failure (in the existing design, the spray system activation fills the cavity with water).
- The reactor sumps are filled with water before the vessel failure.
- In case of vessel failure after core melt, the corium falls and spreads in the dry vessel cavity and optionally in an adjacent area.
- After complete spreading, some triggers are passively activated, allowing water from the sumps to submerge the spread corium. This water allows the corium cooling and its stabilization.

Figure 4: Envisaged modifications to avoid concrete basemat melt-through.

Envisaged modifications to avoid concrete basemat melt-through



Source: IRSN (2017b)

umweltbundesamt

After the review of the principle of these modifications, IRSN has highlighted that this strategy reduces significantly the possibility of containment failure by steam explosion in a flooded vessel cavity and is a good compromise between efficiency and feasibility for the ex-vessel corium stabilization.

However, a several questions remain:

- The size of the spreading area has to be further discussed in accordance with appropriate safety criteria (e.g. thickness of basemat erosion or integrity of the steel liner for the 900 MWe reactors)
- Some design features have still to be defined (e.g. passive trigger system to activate corium flooding by water from the containment floor)
- New instrumentation is needed for the water level in the containment

IRSN pointed out: The final studies of these modifications will be analyzed during the next steps of the safety review process. (Discussion about the coolability of the corium see below)

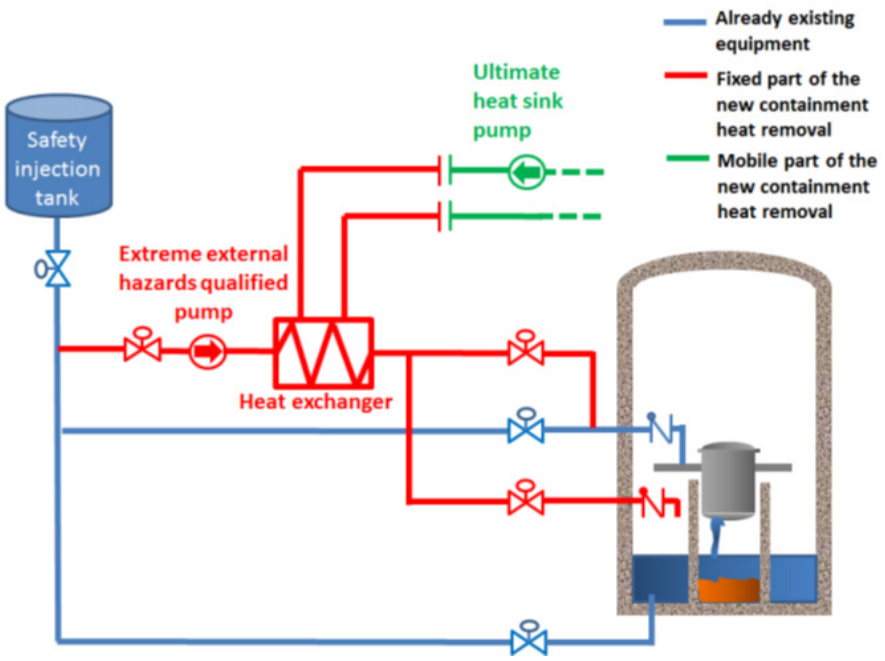
Modification to remove the decay heat from the containment without opening the emergency containment filtered venting system (EFVCS)

In order to allow the possibility to remove the decay heat from the containment without opening the EFCVS, EDF intends to implement a containment heat removal system (called EAS-u) composed of:

- A fixed circuit (located in the fuel building).
  - A pump qualified to extreme external hazards conditions and SA situations;
  - An injection line connected to the cold leg of the primary coolant circuit and another one feeding the sumps of the reactor containment building;
  - A suction line connected to the safety injection tank (direct injection) and another one pumping in the sumps of the reactor containment building (recirculation);
  - A heat exchanger;
  - Actuators enabling the disposal activation from the control room.
- A “cooling mobile circuit” (ultimate heat sink) composed of a mobile pump and hoses directly drawing up in the heat sink and lined on the heat exchanger by the EDF rescue team – FARN.

Figure 5: Containment heat removal disposal (preliminary).

Containment heat removal disposal (preliminary)



Source: IRSN (2017b)

umweltbundesamt

After the review of the principle of this modification, IRSN has concluded that the new disposal intended by EDF is satisfactory in principle and should enable to remove the decay heat from the containment. However, a lot of issues have to be resolved:

- An appropriate instrumentation is important to avoid any excessive pressure or temperature when activating the new circuit
- The possibility of circuit leakage during operation in SA conditions has to be considered with specific provisions (leakage detection, contaminated liquid management, reliable isolation valves…)
- Rescue team FARN activation criteria are important to install the mobile ultimate heat sink in due time (to avoid containment over-pressurization) with margins.

IRSN concluded the final studies of this modification and its qualification to severe accident conditions will be analysed during the next steps of the safety review process.

3.1.1.4 Severe Accident phenomena

In this section the severe accident phenomena which could endanger the containment integrity during a severe accident are briefly described.

Phenomena liable to result in early containment failure

Direct containment heating (DHC)

In France measures have been taken to avoid a high-pressure core melt accident (as in other countries), given the potential consequences of this type of accident, notably in the event of direct containment heating. (IRSN 2015a)

The best way of avoiding or limiting the effect of DCH is to intentionally depressurise the RCS. This can be achieved by opening the pressuriser steam relief valves. The severe accident (SA) operating procedure on the reactors in service requires depressurisation of the primary system by opening the pressuriser relief lines immediately on entry into the SA situation. A hardware modification (integration of a bistable control accessible from the relaying room using a new independent Mobile Safety Means) to enhance the reliability of relief valve opening, decided before the Fukushima Daiichi NPP accident, will be applied to all the reactors until the next 10-year outage of each reactor.

As part of the 4th PSR, EDF is reinforcing the installations by changing the valve heads of the pressurizer to increase their low pressure water discharge capacity primary. This modification consists in increasing the low-pressure discharge section at the opening. (EDF 2018b)

For comparison: In the EPR, the primary system is depressurised by two redundant primary system discharge lines. The operator has one hour after entry into the SA situation to open these lines, which are supplied by 24-hour batteries. In the case of the EPR, design provisions have been made aiming to “practically eliminate” high-pressure core melt accidents. (IRSN 2015a)

Fuel Coolant Interaction (FCI) and steam explosion

Fuel coolant interaction (FCI) occurs in different phases of a severe accident. In the in-vessel phase, molten core materials relocate into the water-filled lower plenum of the RPV. This leads to potentially violent thermal interactions between the fuel and coolant that, in the extreme case, might have an explosive nature (in-vessel steam explosion). This energetic event could endanger the containment integrity if the energy released by the in-vessel steam explosion accelerates a liquid slug of core melt towards the RPV head. When the energy is sufficient to lift off the upper head, the upper head is subsequently accelerated towards the containment ceiling and causes a large containment failure. Lower head failure and the failure of the RCS pipes and steam generator tubes may occur instead.

In the ex-vessel phase, FCI may take place in the reactor cavity provided that there is water present. A violent FCI (ex-vessel steam explosion) has the potential to endanger the structural integrity of the reactor cavity.

Steam explosion is a complex phenomenon induced by the very fast transfer of heat from a hot fluid (melt) and vaporisation of a volatile second fluid (the coolant). A significant amount of energy can also come from the oxidation of metallic components that have a strong reaction heat, such as zirconium, which in turn may endanger containment leaktightness. Even in the case of no cavity/containment failure there is a risk that the functionality of the melt retention capability is reduced.

Furthermore, FCI can also take place in the core catcher device when the melt is flooded. Whilst this is not a violent FCI there is, nevertheless, a possibility of containment failure due to the pressure spikes. (ASAMPSA 2013)

With the above-mentioned modification to avoid basemat melt-through, the risk of ex-vessel steam explosion could be limited. However, currently, the flooding of the reactor pit is one of the measures taken or envisaged to limit the consequences of a core melt accident in the operational reactors, the risk of the containment rupturing as a result of a steam explosion in the reactor pit must be assumed.

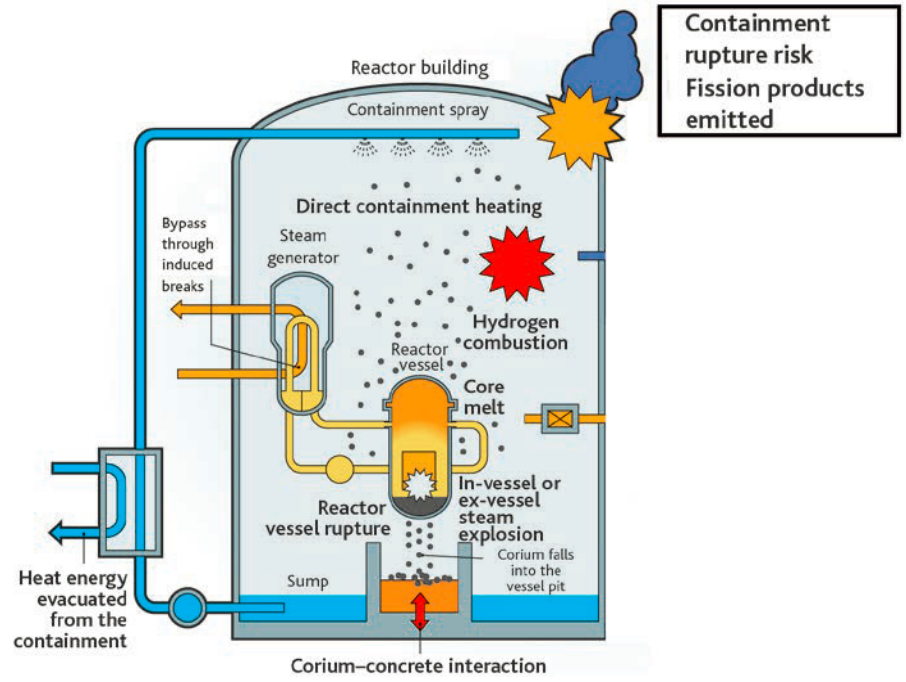
For comparison: In the case of an EPR, the risk of a steam explosion in the reactor pit must be “practically eliminated” by setting up measures guaranteeing that the pit does not contain any water at the time of the corium melt. (IRSN 2015a)

Hydrogen risks and means of mitigating their consequences

Research and development on the hydrogen risk have produced a number of results reinforcing the decision to install passive hydrogen recombiners in all French nuclear power plants. Studies of core melt accident scenarios in the case of the existing reactors and the EPR have shown that despite the installation of recombiners, it is difficult to prevent, at all times and locations, the formation of a combustible mixture potentially resulting in local flame acceleration.

Furthermore, the events that occurred at the Fukushima Daiichi nuclear power plant have shown that the R&D studies must be continued in order to advance the state of knowledge of hydrogen risk phenomena.

Schematic diagram of the physical phenomena



Source: IRSN (2015a)

umweltbundesamt

Figure 6: Schematic diagram of the physical phenomena occurring during direct heating of the gases in the containment.

Coolability of corium and basemat melt through

On the operating reactors, reflooding the corium in the vessel or injecting water into the reactor pit via the perforated vessel to keep the corium flooded limits the risk of basemat melt-through, or failing this, delays its occurrence. However, this strategy is accompanied by the risk of steam explosions. The SAMG defines the water injection conditions, particularly with respect to the risks of early loss of containment.

Stabilisation of the situation in the vessel necessitates restoring a means of injecting borated water into the primary cooling system within a sufficiently short period of time to avoid vessel rupture. For its operating reactors, EDF envisages different possibilities for retaining the corium in the vessel in a severe accident situation, using existing systems that are not specifically designed for managing accidents with core meltdown, and depending on their availability. Following the stress tests, EDF planed to equip the reactor coolant system injection means (hardened safety core pump) backed-up by an Ultimate Backup Diesel Generator.

Maintaining the corium in the vessel avoids the ex-vessel corium-concrete interaction phase and thus contributes to the goal of maintaining containment integrity.

However, achieving melt retention and cooling in the RPV by water injection alone after the onset of melt formation is not guaranteed. Further, water injection will yield oxidation of remaining non-oxidized material and hydrogen production thus increasing the risk of hydrogen combustion in the containment.

IRSN believe that an in-vessel retention (IVR) strategy for the 900 MW reactors based both on in-vessel cooling by water injection and ex-vessel cooling by reactor pit flooding (flooding can be made voluntarily or not and may take few hours) is too uncertain and presents, with the actual knowledge of fuel-coolant interaction, unacceptable risks. It presents “unacceptable” risks as the melt-coolant interaction at RPV failure may result in steam explosion and large early radioactive releases. (IRSN 2015c)

EDF will install on each reactor a system for preventing basemat melt-through in the event of reactor basement melt-through. This system is based on dry spreading of the corium followed by passive flooding of the corium with the water from the sumps.

According to EDF (2018b), the corium is spread after the vessel is perforated in the reactor pit and in the RIC room. Cooling of the corium and evacuation of residual power in the long term are provided by the EAS-u system. According to EDF, this solution, in principle, is similar to the one used on the EPR (core-catcher).

The coolability of the corium in the ex-vessel phase is subject to large uncertainties. The geometry of the 900 MW reactor cavity bottom consists of a circular cylinder of inner radius 2.6 m, sided by a rectangular area facing the in-core Instrumentation System Room – RIC), whose dimensions are approximately 4.0 m x 2.6 m. Thus, the total area of reactor pit and RIC room is 31.6 m². Referring to the indicative figure of 0.02 m²/MWth this translates to a necessary area of approximately 55 m² for the 900 MWe reactor. Consequently, the coolability of the corium is unlikely (ASAMPSA 2013)

A further necessary precondition is the continuous availability of water and the removal of steam. However, in case of the 900 MWe reactors both is not assured.

For comparison: For the Flamanville EPR, the core catcher is intended to collect, cool and stabilise the corium. Prevention of basemat melt-through is thus based on a reactor pit and a core catcher that are both dry when the corium arrives, on the collection and spreading of the corium and on its passive cooling after spreading. In the longer term, the containment heat removal system (CHRS) in the reactor building enables the residual power to be removed from the corium. (ASN 2016)

Risk of reactor containment leak-tightness fault

For the reactors in service, confirmation of the isolation of the containment penetrations is required as part of the immediate actions on entry into a severe accident situation. The activity is monitored so that restoration measures can be implemented if necessary. The DUS (ultimate back-up diesel generator set) will enable the train A containment penetration valves to be re-supplied in the event of a station blackout (SBO) situation. The hardened safety core will allow the containment to be isolated.

For comparison: For the EPR, the containment and the peripheral buildings are designed in such a way that there is no direct leakage path from the reactor containment to the environment. (ASN 2016)

3.1.1.5 Possible degradation of the confinement

According to ASN (2016), the number of events relating to confinement has increased slightly. The leak test carried out on the containment of reactor 5 at Bugey NPP in 2011, during the third ten-yearly reactor safety review, revealed a higher leakage rate than previous tests. Although the leakage rate observed during the test meets regulatory criteria, the increase indicates that the containment is changing over time. ASN therefore laid down a requirement that the containment should be leak tested again within five years, rather than waiting until the next ten-yearly leak test. The following pressure tests in October 2015, revealed that the containment's impermeability had deteriorated compared with the 2011 test.

This increase in the leakage rate is thought to be caused by localised deterioration of the metal liner of the containment, which is approximately 6 mm thick. On the basis of the tests and investigations carried out, EDF believes that a likely source of leaks is the area at the bottom of the reactor building, where the base slab of the internal structures meets the truncated part of the containment cylinder. This joint is filled with a petroleum wax enclosed by sealant and covered with a protective metal plate. The removal of the petroleum wax enabled almost all of the metal liner around the joint to be examined using an endoscope camera, but this did not reveal any defects or holes in the liner.

IRSN examined the actions taken by EDF to locate the leak and restore the tightness of the containment. IRSN pointed out, it cannot be ruled out that this defect occurs on the other 900 MWe reactors. EDF has planned to examine the interest of deploying similar actions on the other 900 MWe reactor enclosures. (IRSN 2018)

The reactor remained shut down for the time it took EDF to define and implement a repair method, which ASN authorised on 28th March 2017. Following the repair, further checks and tests enabled EDF to demonstrate compliance with the safety requirements for the coming cycles. ASN gave its consent for restart of the Bugey NPP reactor 5 on 18th July 2017. Containment should be carried out for all 900 MWe reactors in 2020.

3.1.1.6 Time schedule

According to (IRSN 2018), the work associated with the fourth ten-year review is subject to a complex timetable: the changes associated with the fourth review are divided into two groups corresponding to in phases A (at the outage) and B (4 years after the outage).

This schedule takes into account the schedule of reinforcements decided after the Fukushima accident which was separated into 3 phases (1, 2 and 3). The modifications foreseen in phases A and B of the fourth ten-year review aim to allow the installation of the provisions for phase 3 post-Fukushima reinforcements. However, the schedule of phase 3 is still, to date, the subject of exchanges between the ASN, EDF and the IRSN to limit the duration of deployment. (IRSN 2018)

Further delays are possible. Delays occurred to the most important equipment of Phase 2 recently: In February 2019, ASN has decided to modify the commissioning schedule for diesel generator sets for emergency fuel (DUS) given the

difficulties faced by EDF during construction operations. ASN has included this rescheduling, which extended the deadline until 31 December 2020. According to ASN (2019a), only two DUSs at the Saint-Laurent nuclear power plant are operational yet.

All in all, it is not intended to implement all needed modification during the 4th PSR outage.

IRSN also stated, in view of expected additions needed for the study concerning internal and external hazards, that the demonstration cannot be made on some aspects within the deadlines consistent with the VD4 inspection of reactor No. 1 of the Tricastin site. (IRSN 2019)

3.1.1.7 Severe accident management guidelines (SAMGs)

Recommendations specific to France resulting from the ENSREG peer review of 2012 have high-lighted that the French SAMGs do not cover accidents in the spent fuel pools, nor do they include events that could affect several plant units simultaneously. (ASN 2017)

According to ASN (2017), the implementation of the "hardened safety core" shall be accompanied by measures to ensure that the emergency organisation and resources are operational in the event of an accident affecting some or all of the facilities on a given site, which will require the preparation of specific guides relative to the various scenarios considered.

The various documents relative to severe accident management (SAM) will be validated following the usual processes established by ASN and the licensees.

However, the recent OSART missions (Dampierre NPP, 31 August to 17 September 2015, Follow-up, mission 20 to 24 February 2017 and Bugey NPP 2 – 19 October 2017) pointed to major shortcomings regarding the current severe accident management.

According to IAEA (2017d), the scope of the severe accident management guidance at the Dampierre NPP does not systematically address accidents involving multiple units, accidents occurring in reactor shutdown states and spent fuel pool accidents. The mitigation of a severe accident could be challenged without an accident management programme that comprehensively addresses all severe accident scenarios. According to the follow up mission in February 2017, this is issue was not solved completely.

It has to be noted that this issue seems to be generic. The same issue was also noticed during the OSART mission to Bugey, which took please later (October 2017). The OSART team concluded *"The current scope of the severe accident management guidelines does not address severe accidents with an open primary system, multi-unit events or accidents involving spent fuel pools."* (IAEA 2017c)

3.1.1.8 Level-2 Probabilistic Safety Assessments (Level-2 PSA)

A comprehensive Level-2 PSA is an important tool for the identification of plant vulnerabilities. Level-2 PSAs are also used to evaluate measures of the SAMGs. However, as mentioned above, the Level-2 PSA for the 900 MWe reactors is not comprehensive yet.

During the preceding periodic safety reviews (VD3) for the 900 MWe reactors (CP0-CPY), EDF performed:

- Level-1 and 2 PSAs for failures internal to the reactor,
- Level-1 PSAs for fire (CPY series).

After completing its Level 1 PSA, IRSN estimated core melt frequency to be around 7.5 x 10–6 per year and per reactor for all reactor operational states. (IRSN 2015a)

But the existing PSA (level 1 and 2) for the 900 MWe reactors are not exhaustive in terms of coverage, since they only partially take into account internal and external hazards. In addition, uncertainties stem only from quantitative input data and simplifications and assumptions adopted for the design study. A non-exhaustive list would include uncertainties associated with the choices in combining initiating events, supporting scenarios for thermal-hydraulic and neutronic calculations, modelling of physical phenomena and human actions, estimating the reliability of software and equipment, the choice of event trees and probabilistic quantification software. (IRSN 2015a)

The PSA will be extended during the next PSR, the scope is not sufficient. Under the ongoing 4th periodic safety review, EDF is updating or performing:

- Level-1 and 2 PSAs for failures internal to the reactor and the fuel building pool, for fire, internal flooding and earthquakes,
- Level-1 PSAs for internal explosion and external hazards.

3.1.2 Compilation of currently binding European and international safety requirements

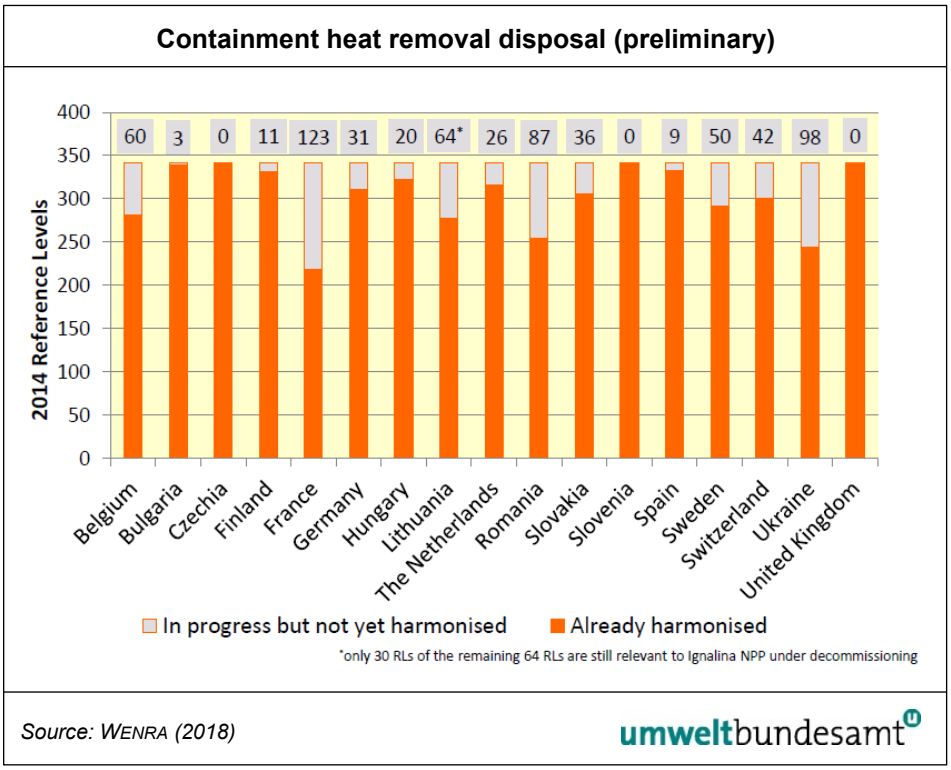
3.1.2.1 WENRA Safety Reference Level

In 2014, the Western European Nuclear Regulators Association (WENRA) published a revised version of the Safety Reference Levels (RLs) for existing reactors developed by the Reactor Harmonisation Working Group (RHWG). The objective of the revision was to take into account lessons learned of the TEPCO Fukushima Daiichi accident. (WENRA 2014)

On 27 October 2014, WENRA published a statement addressing the revised reference levels. With this statement WENRA members committed to implement the RLs into their respective national regulatory frameworks until 2017. (WENRA 2014c)

It has to be noted that, France has not implemented all RL as of the end of 2017. (WENRA 2018)

Figure 7: As of 1 January 2018, the status (regulatory side) reported by WENRA countries.



3.1.2.2 Safety reference level F

A major update of the RLs was the revision of Issue F "Design Extension of Existing Reactors" introducing the concept of Design Extension Conditions (DEC). The term design extension conditions (DEC) has been introduced to achieve consistency with the IAEA SSR-2/1 safety standard (IAEA 2016). In order to provide explanations of the intent of the RLs of Issue F, RHWG developed a Guidance Document for Issue F which was also published by WENRA in 2014. (WENRA 2014b) Some important RLs are discussed in the following section:

Objective of Design Extension Conditions (DEC)

Occurrence of conditions more complex and/or more severe than those postulated as design basis accidents (DBA) cannot be neglected in safety analyses. These conditions shall be investigated as Design Extension Conditions (DEC) so that any reasonably practicable measures to improve the safety of a plant are identified and implemented. (RL F1.1)

RL F1.2 defines two categories of DEC:

- DEC A for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved; and
- DEC B with postulated severe fuel damage.

Selection of DEC

Category DEC A deals with prevention, whereas category DEC B concerns mitigation. Whereas the DEC-B (severe accidents) have been widely assessed and analysed for at least two decades, the DEC-A (BDBA) were analysed in the past only partially – typically only the anticipated transient without scram (ATWS) and station blackout (SBO) were analysed and documented in Safety Analysis Reports.

RL F2.1 stipulates that a set of representative DEC shall be derived and justified based on a combination of deterministic and probabilistic assessments as well as engineering judgment. A wide scope of events and combinations of events exceeding the design basis are to be considered at the beginning of the selection process for DEC A – those events, and combinations of events, which cannot be considered with a high degree of confidence to be extremely unlikely to occur, and which may lead to severe fuel damage. (F2.2)

Events occurring during the defined operational states of the plant shall be covered, including events resulting from internal and external hazards, and common cause failures. A non-exhaustive listing of initiating events for DEC A is provided in the Guidance Document for Issue F, including external hazards. (HIRSCH et al. 2017)

Events extremely unlikely to occur

The concept of “extremely unlikely with a high degree of confidence” constitutes an essential element of the concept of “practical elimination”, as defined by the IAEA. The term “practical elimination” has not been used in the RLs. It is usually applied almost exclusively in the context of severe accidents leading to large or early releases. In the safety reference levels, “extremely unlikely with a high degree of confidence” refers in some cases also to large or early releases; in other cases it refers to severe accidents in the spent fuel pool, and also to certain events.

The demonstration that an accident is extremely unlikely with a high degree of confidence should take account of the assessed frequency of the condition and of the degree of confidence in the assessed frequency. The uncertainties associated with the data and methods should be evaluated, including the use of sensitivity studies, in order to support the degree of confidence claimed. The demonstration should not be claimed solely based on compliance with a general cut-off probabilistic value. Probabilistic and deterministic elements both are required for this demonstration. All analytical methods applied should be validated against the specific phenomena in question, and verified.

Safety analysis of DEC

The selected DEC are subject to DEC analysis. The purpose of this safety analysis can be

(1) to review whether the fundamental safety functions can be guaranteed by existing equipment, or
(2) to identify reasonably practicable measures for enhancing safety.

The safety analysis of DEC shall (F3.1)

a) rely on methods, assumptions or arguments which are justified, and should not be unduly conservative;
b) be auditable, paying particular attention where expert opinion is utilized, and take into account uncertainties and their impact;
c) identify reasonably practicable provisions to prevent severe fuel damage (DEC A) and mitigate severe accidents (DEC B);
d) evaluate potential onsite and off-site radiological consequences resulting from the DEC (given successful accident management measures);

e) consider plant layout and location, equipment capabilities, conditions associated with the selected scenarios and feasibility of foreseen accident management actions;
f) demonstrate, where applicable, sufficient margins to avoid “cliff-edge effects” that would result in unacceptable consequences; i.e. for DEC A severe fuel damage and for DEC B a large or early radioactive release;
g) reflect insights from PSA level 1 and 2;
h) take into account severe accident phenomena, where relevant;
i) define an end state, which should where possible be a safe state, and, when applicable, associated mission times for SSCs.

Ensuring safety function in design extension conditions

In DEC B, the objective is that the plant shall be able to fulfil confinement of radioactive material. (F4.1) SSCs used for DEC shall be adequately qualified to perform their functions for the appropriate period of time. (F.4.2) Plant management under DEC may rely on mobile equipment. Permanent connecting points, accessible under DEC, shall be installed to enable the use of this equipment. (F4.3) A program for inspections, periodic testing and maintenance on mobile equipment should be established, in accordance with the requirements in RL K.

For multi-unit sites, a systematic process shall be used to review all units relying on common services and supplies, to ensure that common resources of personnel, equipment and materials expected to be used in accident conditions are effective and sufficient for each unit at all times.(F4.4) The NPP site shall be autonomous regarding supplies supporting safety functions for a period of time until it can be demonstrated with confidence that adequate supplies can be established from off site. (F4.5) Several WENRA countries stipulate a duration of 72 hours for this period of time.

Regarding the removal of the residual heat from the core and the spent fuel, there shall be sufficient independent and diverse means available, including necessary power supplies. At least one of these means shall be effective after events involving external hazards more severe than design basis events. (F4.7)

Either an alternative ultimate heat sink (including a complete chain of systems providing a link to it) or a chain of independent and diverse systems for using the primary ultimate heat sink (if the primary ultimate heat sink is available for all events within the DEC involving external hazards) should be in place.

Isolation of the containment shall be possible in DEC. For the shutdown states, special attention needs to be given to situations with an open containment. In this case, timely containment isolation should be guaranteed, or measures to prevent core damage with a high degree of confidence made available. Also, in case of events leading to containment bypass, severe core damage shall be prevented with a high degree of confidence. (F.4.8)

Special attention needs to be given to situations with an open containment during certain shut-down states. In this case, a core damage accident could more easily lead to large or early releases. Therefore, timely containment isolation should be guaranteed, or measures to prevent core damage with a high degree of confidence shall be available. Pressure and temperature in the containment shall be managed. (F4.9)

The threats due to combustible gases shall be managed. (F4.10) The threats due to combustible gases (including but not limited to hydrogen) should be understood to cover combustible gases which may originate from the reactor core, spent fuel storage (if applicable) or from the interaction of corium (from reactor core or spent fuel) with concrete. They also include combustible gases which migrate from the building where they were produced, for example into the containment venting system.

A new expectation states that if venting is to be used for managing containment pressure, adequate filtration shall be provided. (F.11)

High-pressure core melt scenarios could lead to the irreversible loss of the confinement function. Therefore, it should be demonstrated that such scenarios are extremely unlikely with a high degree of confidence. (F4.12)

The RLs of Issue F do not require that fuel melt is generally rendered extremely unlikely with a high degree of confidence. Therefore, measures against containment degradation in case of fuel melt are required. Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable. RL F4.13 applies to all situations with molten fuel spreading outside the reactor vessel and can concern for example the risks of steam explosions, direct containment heating or the basemat penetration by the corium. Instability of the reactor building caused by the mass of the water injected into this building as part of efforts to control the molten fuel should also be taken into account.

For the confinement functions, a new RL has been introduced stipulating that in DEC A, releases shall be minimised as far as reasonably practicable. In case of DEC B, any release to the environment shall be limited in time and magnitude as far as reasonably practicable in order to allow sufficient time for protective actions in the vicinity of the plant and to avoid long-term contamination of large areas. (F.14) This RL also implies that the leak tightness of the containment and its penetrations should be maintained in the long term in case of DEC A.

Review of the design extension conditions

Regular assessment of the overall safety of an NPP is required in the Issue “Safety Policy”, in the (new) RL A2.3. A new RL in Issue F emphasizes that this regular assessment has to include the design extension conditions. The main criterion for the implementation of improvements is reasonable practicability. What is reasonably practicable may change over time. Hence, there also is the need for a regular review of DEC.

3.1.2.3 WENRA RL LM (EOP and SAMGs)

Among the issues of the updated WENRA safety RL with the most significant changes is also Issue LM (Emergency Operating Procedures and Severe Accident Management Guidelines). A comprehensive set of EOPs as well as SAMGs shall be provided, covering accidents initiated during all operational states.

Taking into consideration the current the situation, the experience and the recent OSART missions’ results, the following RL of highestconcern forthe French 900 MWe reactors::

- EOPs and SAMGs shall be suitable to manage accidents that simultaneously affect the reactor and spent fuel storages, and shall take potential interactions between reactor and spent fuel storages into account. (LM 2.5)

- Possibilities for one unit, without compromising its safety, supporting another unit on the site shall be covered by EOPs and SAMGs. (LM 2.6)
- EOPs and SAMGs shall be designed so that they are able to be implemented even if all nuclear installations on a site are under accident conditions, taking into account the dependencies between the systems and common resources. SAMGs shall be developed in a systematic way using a plant specific approach. SAMGs shall address strategies to cope with scenarios identified by the severe accident analyses for DEC. (LM 2.7)
- EOPs and SAMGs shall be kept updated to ensure that they remain fit for their purpose. (LM 5.1)
- Control room staff shall be regularly trained and exercised, using full-scope simulators for the EOPs and simulators, where practicable, for the SAMGs. (LM 6.1)
- The transition from EOPs to SAMGs for management of severe accidents shall be regularly exercised. (LM 6.3)

3.1.2.4 Guidance to Article 8a of the EU Nuclear Safety Directive

On the basis of nuclear stress tests carried out in 2011 and 2012, the lessons learned from the Fukushima nuclear accident and the safety requirements of the Western European Nuclear Regulators Association (WENRA) and the International Atomic Energy Agency (IAEA), the EU amended its Nuclear Safety Directive (NSD) in 2014. The amended Directive requires EU countries to give highest priority to nuclear safety at all stages of the lifecycle of a nuclear power plant. This includes ensuring significant safety enhancements for old reactors.

The main outcome of the new NSD for existing plants is Art. 8a:

(1) Member States shall ensure that the national nuclear safety framework requires that nuclear installations are designed, sited, constructed, commissioned, operated and decommissioned with the objective of preventing accidents and, should an accident occur, 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 radioactive releases that would require protective measures that could not be limited in area or time.

Member states shall ensure the objective set out in paragraph 8a (1) is used as a reference for timely implementation of reasonably practicable safety improvements to existing nuclear. (Art. 8a (2))

ENSREG invited WENRA to provide guidance on Art 8a of the Nuclear Safety Directive – *"timely implementation of reasonably practicable safety improvements to existing nuclear power plants"*. This guideline was published in June 2017 (WENRA 2017). Some important statements and explanations are described in the following section.

Proportionality and Role of Cost

Being "proportionate" is a common aim of WENRA members and is a strong element in deciding what is or is not reasonably practicable. A strong feature of being proportionate will be that the greater the shortfall, the more needs to be done to identify and implement measures to remove or reduce it. In some in-

stances, licensees may claim that a particular measure is too costly and therefore not reasonably practicable. In some WENRA countries, the regulator may be prepared to listen to such arguments, in others the regulator does not take account of costs, though in the event of dispute the courts may take cost into account. According to WENRA (2017), claims that a licensee can't afford a reasonably practicable improvement are not accepted.

Defence in Depth

The guideline highlighted that all levels of defence in depth should be considered when considering safety improvements. (See also chapter 2) Important is also enhancing independence between different levels of defence in depth. (WENRA 2017)

PSR and Continuous Improvement

The guidance also emphasized the need for continuous improvement. Despite the important role that PSR has in continuous improvement, there is a need for improvements can also occur anytime between PSRs. PSA is helpful in identifying areas of plant design or operation where improvement will provide most benefit. (WENRA 2017)

In the context of NSD Article 8 a (2) b, i.e. where an existing reactor meets the basic design requirements and its operation can be considered "safe", it is suggested that WENRA members share the following understanding of reasonable practicable safety improvements: *"The concept of reasonable practicability is directly analogous to the ALARA principle applied in radiological protection, but it is broader in that it applies to all aspects of nuclear safety. In many cases adopting modern standards and practices in the nuclear field will be sufficient to show achievement of what is "reasonably practicable". For existing reactors, where a modern standard or good practice associated with new reactors is not directly applicable, or cannot be fully implemented, alternative safety or risk reduction measures (design and/or operation) to prevent or mitigate radioactive releases should be sought and implemented unless the utility is able to demonstrate that the efforts to implement them are disproportionate to the safety benefit they would confer. The degree of rigour and confidence in the outcome of such a demonstration should take account of nature and scale of the shortfall to modern standards that the measure would have addressed."*

WENRA (2017) recommends regulators should have a process in place that considers the following points when deciding if a licensee has done all that is reasonably practicable to meet Article 8a for existing reactors:

- Has the licensee a sufficiently rigorous process to identify shortfalls in preventing and mitigating radioactive releases?
- Is the process shown to be adequate? (e. g. identifies the modern safety standards, encompasses all of the faults and hazards that could lead to a release, all modes of operation, includes Design Extension Conditions (DEC).)
- Has the licensee considered what could be done to remove or reduce the shortfalls? (this should cover all levels in defence in depth that could contribute to prevention or mitigation of radioactive releases, and not be restricted to the specific technology that a new reactor uses to meet the modern safety standard)
- Has the licensee taken due account of national and international practices?

- Of the reasonably practicable options available to reduce a shortfall is the one selected that gives the largest safety benefit?
- Where an option is considered not reasonably practicable has the licensee provided an adequate justification that the measure is disproportionate taking account of the nature and scale of the shortfall?
- Has the licensee considered alternative measures to address the shortfall?
- Has the licensee taken account of the time for implementation in the selection process?
- Do the licensee's processes embrace continuous improvement as well as PSR led improvement?

3.1.2.5 Safety Objective for new NPPs – Benchmark for LTO

The "Safety Objectives for New Power Reactors" published by the reactor harmonization working group (RHWG) Western European Nuclear Regulator's Association (WENRA) can be seen as the state of the art. These safety objectives, formulated in a qualitative manner to drive design enhancements for new plants, should be also "used as a reference for identifying reasonably practicable safety improvements for 'existing plants in case of periodic safety reviews". (WENRA 2010) In March 2013, the WENRA RHWG published a report, which sets out the common positions on the selected key safety issues. (WENRA 2013)

The most ambitious safety objective is to reduce potential radioactive releases to the environment from accidents with core melt. (Safety objective O3) Accidents with core melt which would lead to early releases without enough time to implement off-site emergency measures or large releases which would require protective measures for the public that could not be limited in area or time have to be practically eliminated.

Even though the probability of severe accidents with an early and/or large release for existing plants is estimated to be very small, the damage caused by these accidents is very large. Therefore, the risk of existing NPP for the public is relative high and has to be reduced urgently. Furthermore, the frequency of occurrence of severe accidents, calculated on the basis of the failure rates in all assessed event scenarios, is afflicted with high uncertainties. Technical improvements which are highlighted by WENRA to meet this safety objective are mainly substantial design improvements of the containment.

In their position statement on safety objectives for new nuclear power plants, WENRA members have stated that the safety objectives for new nuclear power plants should be used as a reference for identifying reasonably practicable safety improvements for […] existing plants during periodic safety reviews".

WENRA concluded on LTO: In periodic safety reviews for existing reactors, WENRA safety objectives for new nuclear power plants and other relevant modern standards should be used as a reference with the aim of identifying reasonably practicable safety enhancements. (WENRA 2011)

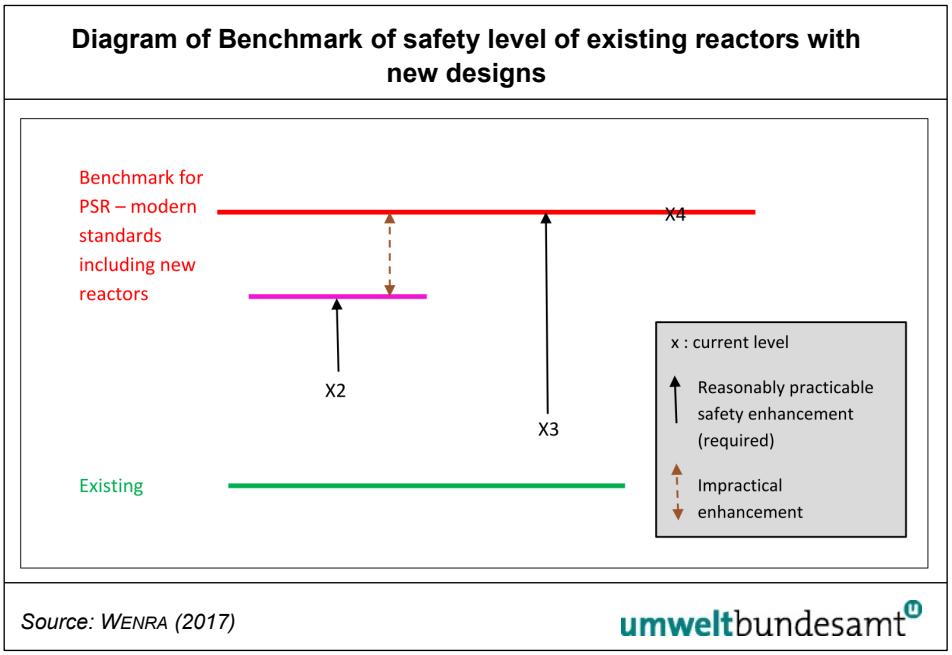


Figure 8: Diagram of Benchmark of safety level of existing reactors with new designs.

As for the horizontal lines:

- The green (lower) line represents WENRA SRLs, and the "X" represent illustrative levels for a variety of safety issue;
- The red (upper) line represents modern standards, including but not restricted to WENRA's new safety objectives, and is the bench mark for comparison in a PSR;
- The green and red lines may in some cases be at the same level (e.g. safety management);
- Those "X" below red line are safety issues that have to be compared to modern standards.
  - In some of these cases it will be reasonably practicable to enhance safety to reach the targets (redline) as in "X3";
  - In some cases, e.g. "X2", it will be reasonable to enhance safety to a level represented by the (purple) line, but further enhancement toward the benchmark is not reasonably practicable;
  - In other cases there may be no identifiable reasonably practicable option for enhancement;
- The "X4" represents these cases where the existing situation is already meeting the modern standard.

3.1.2.6 Demonstration of practical elimination

The fourth level of defence in depth was developed, implying the implementation of design provisions aimed at limiting the consequences of accidents with reactor core melt. However, in some core melt situations which can occur theoretically, it appeared impossible to implement realistic provisions that would reduce the radiological consequences at an acceptable level and to demonstrate their robustness. For this reason, the concept of "practical elimination" was introduced during the 1990s.

The most recent international definitions, particularly those issued by WENRA and the IAEA, state that "practical elimination" should be applied to core melt situations likely to lead to early or large releases (IAEA 2016, WENRA 2010), thus widening the range of situations this applies to.

The concept of 'practical elimination' is to be considered as part of a general approach to safety and its appropriate application as an enhancement of defence in depth. The 'practical elimination' is achieved by prevention of the conditions that could lead to an early radioactive release or a large radioactive release.

As a first step for the implementation of design provisions for the practical elimination of undesired conditions it is necessary to identify what are these conditions and then for each of them specify the design provisions.

The accident sequences that have a potential to lead to early or large releases involve both severe damage of the reactor core and the loss of the containment integrity or containment by-pass. Early or large releases could also be caused by severe damage of spent fuel that is in storage or in transfer outside the reactor containment.

The consideration of severe accidents should be aimed at practically eliminating the following conditions (IAEA 2016b):

- *"Severe accident conditions that could damage the containment in an early phase as a result of direct containment heating, some steam explosions or large hydrogen detonation;*
- *Severe accident conditions that could damage the containment in a late phase as a result of basemat melt-through or containment excessive pressure;*
- *Severe accident conditions with an open containment – notably in shutdown states;*
- *Severe accident conditions with containment bypass, such as conditions relating to the rupture of a SG tube or an interfacing system LOCA".*

Some of these categories entail very severe challenges to the integrity of the physical barriers for radionuclide retention and require specific and very strong design and operation provisions for their practical elimination. The technical measures to prevent each of these situations from occurring need to be provided and their effectiveness needs to be analysed. None of the phenomena mentioned above can be overlooked on the arguments on low likelihood but credible research results and dedicated means to eliminate the identified risks are necessary to support the safety claims.

Extremely unlikely conditions

Although probabilistic targets can be set, 'practical elimination' cannot be demonstrated by showing the compliance with a general probabilistic value. No probabilistic value can be accepted as a justification for not implementing reasonable design or operational measures. The low probability of occurrence of an accident with core melt is not a reason for not protecting the containment against the conditions generated by such accident. The "practical elimination" can be demonstrated by deterministic and/or probabilistic considerations, taking into account the uncertainties due to the limited knowledge of some physical

phenomena. It is stressed that “practical elimination” cannot be demonstrated by compliance with a general “cut-off” probabilistic value.”

Furthermore, when claiming that a particular accident condition of those described earlier was practically eliminated with probabilistic arguments, the rule applies that the cumulative contribution of all the different cases must not exceed the target for large or early release frequency established by the regulatory body.

3.1.2.7 Concept to consider cliff-edge effects

The concept of “cliff edge effects” appears in the IAEA Safety Standards in the Safety Requirements for Nuclear Power Plant Design, in 2000. They required that the safety analysis using the probabilistic approach shall provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behaviour will be prevented. In the nuclear safety framework, an additional and more important issue is the consistent approach needed for considering external hazards in the context of plant states, specifically design basis and design extension conditions. The new IAEA Design Requirements SSR-2/1 introduced new terminology in this respect, it postulated that the transition between “Accident Conditions” and “Beyond Design Basis Accidents” does not involve cliff edge effects.

After the publication of the new Design Requirements SSR-2/1, the IAEA Secretariat perceived the need to prepare a Technical Document titled “Considerations on the Application of the IAEA Safety requirements for design of NPPs” (IAEA 2016b).

Within the analysis of DEC, cliff-edge effects should be identified and a sufficient margin to avoid such effects should be demonstrated wherever applicable. Different kinds of margins may have to be considered, depending on the nature of the DEC. For example, for multiple failure events, the margin could be seen as the capacity of required SSCs to achieve functional capability beyond their design basis, or as the number of additional failures for which it remains possible to avoid severe fuel damage. For certain multiple failures such as total SBO, the margin could be expressed in terms of the period of time available for counter-measures. For events related to reactivity or loss of coolant, the margin could be expressed in terms of fuel temperature or enthalpy release. For external hazards within DEC, margins could be expressed in terms of frequency of severity.

3.1.2.8 ENSREG recommendations

In the framework of the stress tests, each regulator issued a National Action Plan to remedy the identified shortcomings. ENSREG decided to produce a consistent compilation of peer review recommendations and suggestions to assist the preparation or review of national action plans by national regulators. ENSREG (2012)

The compilation of recommendations addressing severe accident management that is of the most importance for the French 900 MW because they are not listed in this chapter:

Provisions for ensuring equipment resistance to severe accidents

Having in place adequate hardware provisions that will survive external hazards (e.g. by means of qualification against extreme external hazards, storage in a safe location) and the severe accident environment (e.g. engineering substantiation and/or qualification against high pressures, temperatures, radiation levels, etc.), to perform the selected strategies. (3.3.2)

Severe accident management guidelines (SAMGs)

…., the enhancement of SAMGs taking into account additional scenarios, including, a significantly damaged infrastructure, including the disruption of plant level, corporate-level and national-level communication, long-duration accidents (several days) and accidents affecting multiple units and nearby industrial facilities at the same time. (3.3.4) and the validation of the enhanced SAMGs. (3.3.5)

The extension of existing SAMGs to all plant states (full and low-power, shutdown), including accidents initiated in SFPs. (3.3.8)

Severe accident simulation exercises and SAM trainings

Exercises aimed at confirming the adequacy of SAM procedures and organizational measures, including extended aspects such as the need for corporate and nation level coordinated arrangements and long-duration events. (3.3.6)

Regular and realistic SAM training exercises aimed at training staff. Training exercises should include the use of equipment and the consideration of multi-unit accidents and long-duration events. The use of the existing NPP simulators is considered as being a useful tool but in need of enhancement to cover all possible accident scenarios. (3.3.7)

Presence of hydrogen in unexpected places

The preparation for the potential for migration of hydrogen, with adequate countermeasures, into spaces beyond where it is produced in the primary containment, as well as hydrogen production in SFPs. (3.3.10)

Level-2 Probabilistic Safety Assessments (Level-2 PSA)

A comprehensive Level 2 PSA as a tool for the identification of plant vulnerabilities, quantification of potential releases, determination of candidate high-level actions and their effects and prioritizing the order of proposed safety improvements. Although PSA is an essential tool for screening and prioritizing improvements and for assessing the completeness of SAM implementation, low numerical risk estimates should not be used as the basis for excluding scenarios from consideration of SAM, especially if the consequences are very high. (3.3.15)

Studies relative to severe accidents

Performaning additional studies to improve SAMGs. Examples of areas that could be improved with further studies include (3.3.16):

- The availability of safety functions required for SAM under different circumstances.
- Accident timing, including core melt, reactor pressure vessel (RPV) failure, basemat melt-through, SFP fuel uncovery, etc.
- PSA analysis, including all plant states and external events for PSA levels 1 and 2.

- Radiological conditions on the site and associated provisions necessary to ensure MCR and ECR habitability as well as the feasibility of AM measures in severe accident conditions, multi-unit accidents, containment venting, etc.
- Phenomena associated with cavity flooding and related steam explosion risks.
- Engineered solutions regarding molten corium cooling and prevention of basemat melt-through.
- Severe accident simulators appropriate for NPP staff training.

3.1.3 Compilation of deviations from the essential safety requirements

Severe accidents (SA) were not considered at the design stage of the French 900 MWe reactors. As a result of previous PSRs, equipment and measures for the SA management were implemented, the EU stress tests however revealed several shortcomings, the necessary improvements have been defined with a view to continuing operation of the reactors beyond forty years, further improvements are envisaged to meet the ASN´s objectives for the life time extension.

After performing the PLE program, a considerable gap between the safety level of the 900 MW reactor and the EPR will persist.

After performing the PLE program, a gap will remain between the safety level of new reactor designs (e.g. EPR) and of the 900 MWe reactors, given the significant design differences such as the number of backup systems trains, the geometrical arrangement of the containment and adjacent buildings, the protection of the spent fuel pools building and the devices for core melt accidents.

For third-generation reactors, core melt accidents are considered in the initial design of the reactors, the measures taken for these reactors cannot all be applied in practice to second-generation reactors. It is a matter of fact, that the 900 MWe reactors cannot reach the EPR safety level for prevention and mitigation of severe accident, as some specific EPR features cannot be implemented for the 900 MW reactors.

Thus, after implementation of all proposed modification and measures to improve the SAM, a gap between the safety level of the 900 MW reactors and the EPR will persist.

The scope of the PLE program concerning core melt accidents is not in compliance with safety requirements.

Safety analyses for the 900 MWe reactors have to identify all possible improvements. EDF intends to close the existing gap regarding severe accidents mainly with modifications for low pressure core melt conditions. EDF's work focused on modifications of heat removal without opening the filtered venting devices and stabilization of the corium on the basement.

This is not in compliance with modern safety requirement and safety objectives for new reactor designs (e.g. EPR). Because one safety objective for EPR is that accident situations with core melt that would lead to large or early releases have to be “practically eliminated”. If they cannot be considered as physically

impossible, design provisions have to be taken to avoid their occurrence. This objective applies notably to high pressure core melt sequences.

However, even though this objective has been largely addressed by the implemented or envisaged modifications for the 900 MW reactors, there are remaining issues associated to uncertainties in the studies including effects of an ex-vessel steam explosion, effects of an uncontrolled injection of non-borated water during accident progression, risk for hydrogen. For high pressure core melt sequences only very limited modifications are foreseen in the PLE program. (IRSN 2017a)

The consideration of severe accidents should be aimed at practically eliminating severe accident conditions that could damage the containment in a late phase as a result of basemat melt-through or containment excessive pressure as well as in an early phase (as a result of direct containment heating, steam explosions or large hydrogen detonation).

To avoid direct containment heating (DCH), the severe accident (SA) operating procedure on the 900 MW reactors requires depressurization of the primary system by opening the pressurizer relief lines immediately on entry into the SA situation. Design improvements for this issue are not foreseen.

Note: With the envisaged modification to avoid basemat melt-through, the risk of a ex-vessel steam explosion could be limited. Currently, the flooding of the reactor pit is one of the measures taken or envisaged to limit the consequences of a core melt accident, however, the risk of the containment rupture as a result of a steam explosion in the reactor pit is not excluded.

Demonstration of adequate safety level is not in compliance with current safety requirements

EDF points to the reduction of the risk of specific accident situations, however the demonstration of safety is often based on low probabilistic risk values.

According to WENRA and IAEA requirements, the fulfilment of a probabilistic value cannot be considered as a justification for not implementing reasonable design or operational measures.

To meet current safety objectives the concept of “practical elimination” has to be used: The practical elimination from consideration of accident situations that could lead to large or early releases has to be demonstrated by deterministic considerations supported by probabilistic considerations, taking into account the uncertainties due to the limited knowledge of some physical phenomena.

Even though the probability of severe accidents with an early or large release for 900 Mw reactors is estimated to be very small, the damage caused by these accidents is very large. Furthermore, the frequency of occurrence of severe accidents, calculated on the basis of the failure rates is afflicted with high uncertainties. The demonstration that an accident is extremely unlikely with a high degree of confidence should therefore not only take account of the assessed frequency of the condition and but also of the degree of confidence in the assessed frequency.

To meet modern safety standards, the uncertainties associated with the data and methods should be evaluated, including the use of sensitivity studies, in order to underwrite the degree of confidence claimed. But, the demonstration of

adequate safety level for the 900 MW reactors does not sufficiently address the issue of uncertainty.

Long-term stabilization of the molten core and heat removal without venting is currently not and will not be guaranteed after the PLE program

The device to avoid basemat melt-through by molten core after RPV failure is not implemented yet. Additionally, there are doubts about the efficiency of this device; especially the corium coolability during molten core concrete interaction is not demonstrated yet. The (sufficient) thickness of the basemat and the size of the spreading area is still an issue.

Studies have to demonstrate the feasibility and effectiveness of this device, which would have important differences with the EPR core catcher. The limitation of the spreading area due to building constraints impede the realizing of the new device. Integrity of the basemat thickness and steel liner during a core melt accident and thus the confinement of the radioactive substance is not assured yet. Necessary design features have to be defined yet (e.g. passive trigger system and instrumentation).

From the view of the current knowledge, a failure of the containment function cannot be excluded after implementation of the modification for the stabilization of molten.

The reliability of the envisaged modification for heat removal without venting during a severe accident is also not proven yet.

WENRA safety reference level F (design extension conditions) not applied completely

To ensure containment integrity, the objective, scope and approach of the WENRA reference level F has to be fully applied. This is not the case for the 900 MW reactors:

The safety analyses for core melt accidents do not rely on methods, assumptions or arguments which are justified; take into account uncertainties and their impact; demonstrate, sufficient margins to avoid “cliff-edge effects” that would result in unacceptable consequences; reflect insights from PSA level 1 and 2; take into account severe accident phenomena. (F3.1)

Ensuring confinement of radioactive substances has following deficits:

- There is not at least one mean available that is effective after events involving extreme external hazards to remove of the residual heat from the core and the spent fuel. (F4.7) Furthermore the design and capabilities of these means are still under discussion.
- Measures to manage pressure in the containment are not appropriate yet and it remains unclear whether they will be adequate after the PLE program’s implementation (F4.9).
- The dangers arising from hydrogen explosions are not managed sufficiently. No decision taken about further actions. (F4.10)
- The filtered venting to be used for managing containment pressure doesn’t provide adequate filtration to limit the need for emergency protective measures

for the population in the plant's immediate vicinity. (F4.11); its seismic reinforcement is not appropriate.

- It was not demonstrated that high-pressure core melt scenarios that could lead to the irreversible loss of the confinement function are extremely unlikely with a high degree of confidence. (F4.12)
- According to RL F4.13, containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable. This does not apply to all situations with molten core (e.g. fuel spreading outside the reactor vessel, the risks of steam explosions, direct containment heating or the basemat penetration by the corium.)

All in all, it is not demonstrated that any radioactive release into the environment is as far as reasonably practicable limited to (a) allow sufficient time for protective actions in the vicinity of the plant; and (b) avoid contamination of large areas in the long term (F4.14).

The requirements of Art 8a of the Nuclear Safety Directive and its guidance are not met

To assess if EDF has done or will do all that is reasonably practicable to meet the objective of Article 8a, it is important that EDF explains his procedure to identify shortfalls in preventing and mitigating radioactive releases and measures to remove or reduce the shortfalls. WENRA (2017) points out that this should cover all levels of the defence in depth concept, and not be restricted to the specific technology that a new reactor uses to meet the modern safety standard. EDF has to provide an adequate justification for the case that an option is assessed as not reasonably practicable. According to WENRA (2017), the licensee's argument that a reasonably practicable improvement is unaffordable, is unacceptable.

A systematic comparison with the safety level of the new reactor designs (e.g. EPR) wasn't provided.

According WENRA (2011), the safety objectives for new nuclear power plants should be used as a reference for identifying reasonably practicable safety improvements for existing plants during PSR especially for PLE. A proposal for the comparison is provided.

The overall objective to be used for VD4-900 review, which is to avoid fuel melting and limit radioactive release is consistent with that used for the EPR-FA3. However, the safety requirements to meet this goal are only partly addressed by EDF. EDF´s PLE program lacks a systematic comparison of modern safety standards to illustrate the remaining gap.

Consequences and prevention of cliff-edge effects are not always considered

According to WENRA (2014) and IAEA (2016b), within the safety analysis of DEC, cliff-edge effects should be identified and a sufficient margin to avoid such effects should be demonstrated. For certain accidents, the margin could be expressed in terms of the period of time available for counter-measures. For external hazards within DEC, WENRA recommended to ensure that the higher in-

tensity hazard do not induce cliff-edge effects and identify ways to ensure the availability of safety functions in such a situation. However, according to IRSN (2019), EDF has not analyzed cliff-edge effects for all external events.

Increasing the safety level after the implementation of the Hardened Safety Core is limited, because it is not in compliance with modern safety requirements

The Hardened Safety Core with its important role in preventing but also in mitigating core melt accidents is not realized yet. Furthermore, it is not assured that after implementation:

- the existing SSCs in interface with the hardened safety core (HSC) will meet adequate requirements in terms of resistance to extreme hazards and their induced effects.
- all equipment for the HSC is able to withstand all extreme hazards (e.g. air temperatures);
- the main SSCs of the HSC and their support (such as electrical distribution and switch-gears for example) would be as far as possible:
  - independent from the existing SSCs, to ensure that the HSC constitutes the expected ultimate line of defence and is not affected by the potential failures that may occur on the other parts of the installation,
  - diversified from the existing SSCs to limit the risks of common cause failures.
- the implementation of the HSC functions will require limited local actions by the staff.

Presence of hydrogen in unexpected places is not calculated adequate

One of the most important lessons learnt from the Fukushima accident, having adequate countermeasures ready in case of a possible hydrogen migration, has not been introduce.(ENSREG 2012, recommendation 3.3.10) Because of an error in the models, the risk of hydrogen explosion is not analyzed correct. (IRSN 2019)

Equipment resistance to external hazards and severe accidents is and will not be assured

The EU stress tests revealed that several equipment items required for severe accident management are not qualified for external hazards (e.g. earthquakes). The reinforcement to remedy these shortcomings is still ongoing. However, even after the reinforcement, the seismic resistance of the filtered venting systems will not comply with current safety requirements.

The ENSREG (2012) recommendation to have an adequate hardware provisions that will survive external hazards (…) and the severe accident environment in place to perform the SA strategies is not fulfilled. (3.3.2)

Comprehensive Level-2 Probabilistic Safety Assessment (Level-2 PSA) is still missing

A comprehensive Level 2 PSA including all plant states and external events as a tool for the identification of plant vulnerabilities and to improve SAMGs is recommended by ENSREG (3.3.15) However PSA 2 for all extern hazards this is not done yet and not envisaged in frame of the forth PSR.

The envisaged for time schedule for the PLE program is not adequate

In case, the modification for core stabilization and long-term heat removal can demonstrate the efficiency, industrial challenges associated to the practical implementation on each reactor. According to EDF´s proposal the new equipment will not be available on the reactor remain at the end of the outage of the forth PSR, but four years later. Due to the above-mentioned open questions further delays are possible. Because of the significant weaknesses regarding the SAM, EDF´s time schedule is not adequate. All measures have to be implemented before the restart after the VD4 outage.

Preparation and feasibility of the manual actions needed for SAM are not assured

The FARN should be able to support the plant staff in a severe accident situation after 24 hours, thus it is important that the plant staff is able to cope with a severe accident. The ability to manage complex accident situations including the sufficiency and robustness of the fixed and mobile equipment is still under discussion. But under severe accident conditions, it is very important that the proposed mobile equipment can be put to work as quickly as necessary; to rely to such a large extent on manual actions should be carefully assessed in regard of the consequences of a severe accident.

Despite the fact the actions of the staff are very important, there are also still shortcomings in the area of SAM exercises and trainings. The fulfill-ment of the WENRA safety reference level LM (Emergency Operating Procedures and Severe Accident Management Guidelines, in particular RL 2.5, 2.6, 2.7. 3.3, 3.4, 5.1, 6.1, 6.3) should be ensured before the restart of the plant after the VD4 outage.

The envisaged severe accident management rely to a large extent on manual actions of the staff. It should be carefully analyzed whether in severe accident situations, wether sufficient time is available to realize these measures (otherwise design improvements are necessary.)

The following ENSREG recommendations concerning the preparation and feasibility for severe accident management are not fulfilled yet:

- The extension of existing SAMGs to all plant states (full and low-power, shutdown), including accidents initiated in SFPs. (3.3.8)
- Exercises aimed at checking the adequacy of SAM procedures. (3.3.6)
- Training exercises including the use of equipment and the consideration of multi-unit accidents and long-duration events. (3.3.7)
- The performance of further studies to improve SAMGs including the availability of safety functions required for SAM under different circumstances and accident timing (3.3.16).

Taking into account possible containment degradation and reactor pressure vessel defects

To take into account the observed containment degradation of the Bugey NPP is necessary

- to have a comprehensive understanding of the reason for the increase of the leakage rate over the time,
- to integrate of the assumption of degradation of the containment into safety analysis.

The same should be applied for possible defects of the reactor pressure vessel, because defects have been detected in RPV of the reactors Tricastin 1, Fessenheim 2 and Saint-Laurent-des-Eaux 1.

3.1.4 Results

After performing the PLE program, a considerable gap between the safety level of the 900 MW reactors and the EPR will persist: It is a matter of fact, that the 900 MWe reactors cannot reach the EPR safety level for the prevention and mitigation of severe accidents, as some specific EPR features cannot be implemented for the 900 MW reactors.

The overall objective to be used for VD4-900 review, which is to avoid fuel melting and limit radioactive release is consistent with that used for the EPR. However, the safety requirements to meet this goal are only partly addressed by EDF. A systematic comparison between the safety level of the 900 MW reactors and modern safety standards to illustrate the remaining gap is lacking in EDF´s PLE program.

The scope of the PLE program concerning core melt accidents is not compliance with current safety requirements: EDF intends to close the existing gap regarding severe accidents mainly with modifications for low pressure core melt conditions. For high pressure core melt sequences, only limited modifications are foreseen.

The demonstration of the adequate safety level is not in compliance with modern safety requirements. EDF points to the reduction of the risk of specific accident situations, the demonstration of safety is often based on low probabilistic risk values. However, to meet current safety objectives the concept of “practical elimination” has to be used. The demonstration that an accident is extremely unlikely with a high degree of confidence should take account of the assessed frequency of the condition and the degree of confidence in the assessed frequency. Safety analyses do not address uncertainties appropriate. Consequences and prevention of cliff-edge effects are not always considered

From the view of the current knowledge, a failure of the containment function cannot be excluded after implementation of the modification for the stabilization of the molten core. The reliability of the envisaged modification for heat removal without venting during a severe accident is also not proven yet.

To ensure containment integrity, the objective, scope and approach of the WENRA reference level F (design extension conditions-DEC) has to be applied completely. This is not the case for the 900 MW reactors. Thus, it is not demonstrated that any radioactive release during a core melt accident is as far as rea-

sonably practicable limited to (a) allow sufficient time for protective actions in the vicinity of the plant; and (b) avoid contamination of large areas in the long term.

The Hardened Safety Core (HSC) that shall have an important role for the prevention core melt accidents but also for the mitigation of the consequences of core melt accidents is not implemented yet. Furthermore, it is not assured that after complete implementation, the HSC (and in particular the existing structures, systems and components (SSC) of the HSC) will adequately meet the safety requirements.

One of the most important lessons learnt from the Fukushima accident, the preparation for the potential for migration of hydrogen with adequate countermeasures is not taken yet. Because of an error in the models, the risk of hydrogen explosion is not analyzed correct.

Equipment resistance to external hazards and severe accidents is and will not be assured. The EU stress tests revealed that the several equipment items required for severe accident management are not qualified for external hazards (e.g. earthquakes). The reinforcement to remedy these shortcomings is still ongoing. However, even after the reinforcement, the seismic resistance of the filtered venting systems will not comply with current safety requirements.

The ENSREG (2012) recommendation requiring an adequate hardware provision that will survive external hazards (…) and the severe accident environment in place to perform the SA strategies is not fulfilled.

A comprehensive Level-2 Probabilistic Safety Assessment (Level-2 PSA) as a tool for the identification of plant vulnerabilities and to improve severe accident management guidelines (SAMGs) is still lacking.

Preparation and feasibility of the manual actions needed for SAM are not assured: The severe accident management relies to a large extent on manual actions of the staff. The ability to manage complex accident situations including the sufficiency and robustness of the fixed and mobile equipment is still under discussion. Despite the fact that the actions performed by the staff are very important, in the area of SAM exercises and trainings shortcomings still exist.

Conclusion: For the 900 MW reactors, a core melt accident with a major release is possible today and will be possible after the implementation of the currently envisaged PLE program.

4 SPENT FUEL

4.1.1 Description of the facts

4.1.1.1 Vulnerability of the Spent Fuel Pool

In France, the spent fuel pools of all reactors are not located within the containment structure, but next to it in a separate building with less protection. According to the French nuclear safety authority, at all sites these buildings have a thin metal roof and relatively thin walls (0.3 m) (ASN 2011). Available data about the spent fuel building show that the thickness of the wall in the area of the water basin is about 0.8 to 1 m. Because of the walls' thinness the probability of a severe damage of the spent fuel building by external hazards is relatively high.

The safety design for spent fuel pools in the reactors was even less robust than the safety design for reactors. This resulted from the belief that the risks posed by spent fuel pools were far less severe than those posed by the reactors themselves. Even though spent fuel pools could contain a quantity of fuel several times greater than the quantity in the reactor core, the heat load would be far lower than the core. In the event of a loss of spent fuel pool heat removal, operators would have a significantly longer time to respond and mitigate the situation (days to weeks) before the water in the pool boiled away, the spent fuel became uncovered and began to overheat.

The spent fuel pools of the 900 MW series have a storage capacity of 382 spent fuel assemblies. Taking into consideration the capacity that has to be kept free for a core unloading (157 fuel assemblies), that leaves a maximum of 225 fuel assemblies.

The stress test revealed, the fuel building is not designed to contain the radioactive substances in the event of a pressure rise following a steam release resulting from water boiling in the SFP. In France, as in most countries, nuclear regulators did not require spent fuel pools to be located within a leak-tight, pressure-resisting containment structure comparable to those for the reactor core, because such structures were only needed to withstand the conditions that would occur during a fuel melt accident.

However, this philosophy was put into question by the changing attitude toward the risk of sabotage that took place after the 11 September 2001 attacks in the United States.

As the storage pools of the U.S. reactors are also located outside the reactor containment structure, particular concern was voiced after the 9/11 terror attacks about the vulnerability of spent fuel by terror attacks. A report released in April 2005 by the U.S. National Research Council of the National Academy of Sciences (NAS) found that "successful terrorist attacks on spent fuel pools, though difficult, are possible." Terrorists could breach the concrete walls of a spent fuel pool and drain the cooling water and "if an attack leads to a zirconium cladding fire, it could result in the release of large amounts of radioactive material." (NSA 2006)

The threat of a large breach of the spent fuel pool (after an earthquake) was also highlighted during the Fukushima accident in 2011.

To consider the (radiological) consequences of an attack or extreme hazards it is important to distinguish two different scenarios:

To a): If the basin remains intact, but the pool cooling system fails and water gradually boils off, it will take days or weeks (depending on amount and age of the spent fuel in the pool) until the tops of the fuel assembles are exposed. During this period of time, intervention could provide sufficient cooling of the fuel. In case the entire core has been unloaded into the pool at the time of the attack intervention measures would have to be implemented during a few hours.

To b): An external event resulting in major damage to the building would cause cooling water loss. If the water drains off and refilling of water is not foreseen or possible, very severe radioactive releases begin within hours. This leads to a dangerous challenge: As soon as the water has drained out of the pool, not only the cooling, but also the shielding effect of the water is lost. Fuel that has been extracted only a short time earlier from the reactor would generate a relatively high amount of heat and can reach a temperature of 900 °C within a few hours. At that temperature, the fuel cladding made of zircaloy would burn in the air. The fire is very hot and cannot be extinguished with water. Within the cooling pool it could spread to older fuel assembles that would otherwise not heat up so rapidly. Thus, the entire inventory of the cooling pool could melt. (ALVAREZ 2003)

In this situation, the population would have to be evacuated during an extremely short time.

Spent fuel pools are also vulnerable when the reactor is not in operation, even more so. The most dangerous situation occurs during refuelling when all the fuel has to be unloaded from the reactor core to the spent fuel pool.

Severe damage to the cooling pools would lead to considerable release of radioactive substances. During the storage time of the spent fuel the shorter-lived radionuclides are reduced, in particular the highly volatile iodine-131. However, the inventory of the relevant radionuclide caesium-137 remains high. According to a recent U.S. study, about 75 percent (10-90 percent) percent of the caesium-137 inventory could be mobilized in the plume from the burning spent fuel pool. (HIPPEL 2016)

Airplan crash

The spent fuel buildings at the French NPPs are highly visible and therefore relatively easy targets for an attack from the air. The 900 MW reactors with their spent fuel pools were designed and constructed before the accidental crash of a commercial sized aircraft was conceived as a real threat. No studies about the consequences of a deliberate aircraft crash against a French NPP (reactor building or the building of the spent fuel pool) are available. It is, however, pos-sible to draw conclusions from the results of studies carried out in other coun-tries e.g. Germany and general considerations regarding the possible effects of such an aircraft crash. A generic study commissioned by the German Federal Environment Ministry (BMU) revealed, that even a small commercial aircraft (e.g. an Airbus A320) would cause major damage to the reactor building with a wall thickness of 0.6 to 1 metres. (BMU 2002)

A number of studies investigated special issues connected to the impact of a commercial aircraft against a nuclear power plant to develop protection ofthe next generation of nuclear power plants. A 2010 report concluded from different studies that a wall thickness of roughly two meters is sufficient to prevent the perforation even in the case of the crash of a Boeing-747. (PETRANGELI 2010).

Those facts show that a crash of a large or a midsize aircraft would cause a major damage of the building. Furthermore, it has to be assumed that happens also with a relatively small aircraft (e.g. an Airbus A320) crashing against the building. The relatively thin wall will fail under the commercial-sized aircraft's impact and the spent fuel pool's water rapidly drains and leaves the fuel ex-posed. Due to the complexity of the situation after an airplane crash the per-sonnel would temporarily not have the capacity to conduct intervention measures.

Because the building of the spent fuel pools is directly adjacent to the reactor building, the reactor could be also affected by the same attack. It possible that the vibration of the airplane crash causes damage of the safety systems of the reactor itself; and thus, the staff and later the FARN would have to prevent a core melt accident. Once the spent fuel release has started, these measures would be very complicated and dangerous.

4.1.1.2 Stress test results

According to ASN (2017), the stress tests included an in-depth examination of a major natural hazard's consequences on the systems that can remove the residual heat from the fuel stored in pools, on the integrity of the pools in the fuel building or the reactor building and the systems connected to them, and the risks of storage rack deformation and falling loads.

The conclusions of the analyses have led ASN to issue several orders. (ASN 2016)

- Installation of reinforced instrumentation in the pool for measuring the conditions of the spent fuel pool (temperature and water level) and the radiological atmosphere in the fuel building hall (ECS-20);
- Implementation of additional measures to prevent or mitigate the consequences of a fuel transport package falling in the fuel building on the Bugey and Fessenheim sites (ECS-21);
- Reinforcement of the measures designed to prevent accidental rapid draining of the fuel storage pools (ECS-22);
- Study of the possible measures, in the event of total loss of electrical power supplies and accidental emptying, to ensure the safe positioning of a fuel assembly during handling in the fuel building, before the ambient conditions prevent access to the premises (ECS-23);
- Study of the evolution over time of the fuel and the water present in the spent fuel pool, in situations of emptying and loss of cooling, and presentation of the planned modifications (ECS-24);
- Study of conceivable changes to equipment or operating conditions to prevent uncovering of the fuel assemblies during handling, for example as result of a break in the transfer tube between the pools of the reactor building and the fuel building or in the compartment drainage pipes (ECS-25)

In compliance with ASN's requirement, EDF presented the modifications to be made to its facilities to reinforce prevention of the risk of accidental emptying of the fuel building pool:

- The spent fuel pool level measurement system is in place and electrically backed up by the new generator sets but pending their connection to the ultimate backup diesel generator set. (ECS – 20)
- The Bugey and Fessenheim plants could entail a particular risk of spent fuel pool damage should a fuel transport container fall. At the end of 2012, EDF submitted a study of the consequences of an accident involving the falling of a spent fuel transport package, integrating the extreme situations studied under the stress tests for these two sites. At Fessenheim, the integrity of the basemat is not called into question by the falling of a package. The analyses at the Bugey NPP have resulted in proposing the installation of a hydraulic damper in the loading pit similar to that of Fessenheim, and an energy absorbing system beneath the handling opening. (ECS – 21)
- EDF has redesigned the siphon vacuum breaker on the cooling system delivery pipe to prevent complete and rapid siphon emptying of the pool in the event of rupture of a connected pipe. This modification was carried out on all the reactors before the end of March 2014. Furthermore, an automation of isolation of the cooling system intake line was implemented. (ECS – 22)
- EDF performed a study of the evolution over time of the behaviour of the fuel and the water present in the spent fuel pool, in emptying and loss of cooling situations. The studies submitted describe the kinetics and consequences of a pool boiling emergency. The proposed mitigation measures consist in restoring the water inventory in the pools through water make-up which forms part of the hardened safety core, with the pool then being cooled by a mobile means. (ECS – 24)
- At the end of December 2012, EDF submitted the feasibility studies for handling the case of a breach in the transfer tube. Two types of solution can be used to prevent exposure of the fuel assembly during handling. The detailed studies needed to optimize the choice of the solution are in progress. EDF then initiated a programme to qualify the materials used for the two modifications envisaged to guarantee satisfactory retention of the fluid from a break in the transfer tube. At the end of 2016, none of the two modifications had been definitively adopted. At the same time, EDF is carrying out mechanical strength studies on the transfer tubes with respect to the “hardened safety core” earthquake in order to assess the displacements induced on the civil engineering penetration sleeves. (ECS – 25)

4.1.1.3 Objectives of the forth PSR

For the forth PSR, ASN has set EDF the objective of adopting a continuous safety improvement approach at each review, to take into account the best international practices (particularly the work of WENRA) and the development of knowledge and the rules applicable to similar installations, and new reactors in particular.

However, according to the Fulfillment report, EDF has set itself only the objective of ensuring that the likelihood of fuel assemblies becoming uncovered remains extremely small in the event of inadvertent drainage and loss of cooling. (EDF 2018a)

For purposes of the fourth PSR, EDF is consolidating the fuel building's safety levels in accident conditions by taking the following measures:

- Installing additional equipment to address the risk of inadvertent spent fuel pool drainage: motor-operated valves on the suction side and check valves on the discharge side of the spent fuel pool cooling system;
- Adding a flame-proof system to guard against the risk of fire spreading from one cooling-system pump to another.

EDF (2018a) explained that deterministic analyses proved that safety requirements were met for all postulated initiating events when taking into account the existing measures. Furthermore, a specific assessment showed that the residual heat removal function and the assumed spent fuel pool inventory would not be compromised in the event of an internal hazard.

Probabilistic assessments show that the likelihood of uncovering the fuel assemblies in the event of a) inadvertent drainage and b) loss of spent fuel pool cooling is extremely small (about 10-8 per year and reactor) thanks to the new capabilities of the "hardened safety core" (e.g. replenishment of spent fuel pool inventory) and the response of the FARN.

The installation of a new mobile cooling system has diversified the heat sink and enables plants to restore their spent fuel pool cooling function without reaching boiling point in the event of a loss of the design-basis cooling system. According to EDF (2018a), this type of measure has brought the safety level of 900-MWe reactors closer to that of Flamanville-3 EPR reactors.

According to EDF (2018a), the behaviour of spent fuel pools on the 900-MWe reactor fleet was assessed in accident scenarios used for the Flamanville-3 EPR but not considered in the initial design. This assessment highlighted the robustness of these spent fuel pools.

4.1.2 Compilation of currently binding European and international safety requirements

4.1.2.1 ENSREG recommendations

In the framework of the EU Stress test, ENSREG (2012) recommends the improvement of the robustness of the spent fuel pool (SFP). Examples include:

- reassessment/upgrading SFP structural integrity,
- installation of qualified and power-independent monitoring,
- provisions for redundant and diverse sources of additional coolant resistant to external hazards (with procedures and drills),
- design of pools that prevents drainage,
- the use of racks made of borated steel to enable cooling with fresh (unborated) water without the danger of possible re-criticality,
- redundant and independent SFP cooling systems,
- deployment of additional heat exchangers (e. g. submerged in the SFP),
- an external connection for refilling of the SFP (to reduce the need for an approach linked to high doses in the event of the water falling to a very low level)
- and the possibility of venting steam in a case of boiling in the SFP.

4.1.2.2 WENRA Safety Reference Level F

According to RL F4.1, the plant shall be able to prevent the release of the radioactive material.

WENRA Guidance on Safety Reference Levels of Issue F, requires special efforts to make severe accident in a spent fuel storage extremely unlikely with a high degree of confidence, since measures for sufficient mitigation of severe accident consequences in spent fuel storages could be difficult to realize. Extreme unlikeliness with a high degree of confidence is an element of the concept of practical elimination. To demonstrate extreme unlikeliness with a high degree of confidence, both probabilistic and deterministic elements are re-quired. The demonstration should not be claimed solely based on compliance with a general cut-off probabilistic value. Within the analysis of DEC, cliff-edge effects should be identified and a sufficient margin to avoid such effects should be demonstrated. (WENRA 2014b)

4.1.2.3 Protection according to current safety requirement

For the EPR, the outer shell (doubled-concrete shield) covering both the reactor building and the spent fuel building provides protection against large commercial aircraft or military aircraft crash.

4.1.3 Compilation of deviations from the essential safety requirements

The stress tests revealed several safety deficits for the stored spent fuel pools of the 900 MWe reactors. Most of the necessary back-fitting measures have not yet been implemented. These include the systems of the Hardened Safety Core and the reinforcement of the transfer tubes.

Despite this fact, ASN has ordered EDF to take into account the best international practices (particularly the work of WENRA) and the development of knowledge and the rules applicable to similar installations, and new reactors in particular.EDF has set itself more limited objectives for the spent fuel in the PLE program.

EDF only plans to ensure that the likelihood of fuel assemblies becoming uncovered remains extremely small in a) the event of inadvertent drainage and b) loss of cooling. (EDF 2018a)

A rapid drainage of the SFP because of a failure of the pools' structure is not considered. In EDF's view a rapid drainage of SFP could occur due the operating of the pumps and an automatic shutdown of these pumps has been implemented.

Measures are envisaged to restore the cooling of the SFP after the loss of the power supply and/or ultimate heat sink. With the envisaged measure it is not possible to refill the water in case of the loss of the cooling water due to a leakage in the structures of the spent fuel pool.

As a response to the Fukushima accident, ENSREG (2012) recommends the improvement of the robustness of the spent fuel pools (SFP). This includes among others measures the reassessment/upgrading of SFP structural integrity. However, a reinforcement of the structure of the spent fuel pool buildings or a reassessment is not planned by EDF in the PLE program.

EDF points to the very small likelihood of a severe accident in the SFP. This approach is not in compliance with WENRA requirements. According to WENRA (2014), special efforts are needed to meet the goal that a severe accident in a spent fuel storage becomes extremely unlikely with a high degree of confidence, since measures for sufficient mitigation of the consequences of a severe accident in spent fuel storages could be difficult to realize. The demonstration should not be solely based on compliance with a general cut-off probabilistic value. Both probabilistic and deterministic elements are required for this demonstration.

Furthermore, only internal hazards are analyzed, external hazards are only partly addressed. The consequences of loss of the structural integrity of the spent fuel pools are not included in the demonstration that a severe accident in the spent fuel pool is extremely unlikely. This analyses and possible reinforcement of the structure are needed to comply with the requirement to identify and prevent cliff-edge effects.

After performing the PLE program, there will be a considerable gap between the safety level of the EPR and the 900 MWe reactors: The protection against the deliberate crash of a commercial airliner against the SFP building, provided for in the design on the EPR is not envisaged by EDF for the 900 MWe reactors.

4.1.4 Results

The stress tests revealed several weaknesses of the safety level for the stored spent fuel pools of the 900 MWe reactors. Most of the required back-fittings measures haven't been implemented yet.

However, the most dangerous weakness, the vulnerability of the SFP because of the thin walls will persist for the next 20 years. Improvements are not envisaged in the PLE program. Thus, the 900 MW reactors will not meet the safety standards of the EPR (protection of the spent fuel building against commercial airplane crash).

An external event laeding to a leakage in the spent fuel pool of the 900 MW reactors would cause the loss of the cooling water. Because sufficient measures to refill the pool water are not available an unavoidable severe accident with considerable release of radioactive substances would occur.

5 IMPLEMENTATION OF NECESSARY UPGRADES IN TIME

5.1 Description of the Facts

In France, the lifetime of nuclear power plants is not limited by the permits. Any further operation of a nuclear power plant over a period of 10 years shall be decided by the competent authority on the basis of the results of a periodic safety review, which takes place every 10 years.

The periodic safety review has to deliver results that make it possible to verify if

- the operation of the nuclear power plant complies with the conditions of the permit and
- the respective nuclear power plant carries out active projects in order to continuously increase the safety level with reference to modern safety standards and international recommendations. All reasonably reliable improvements should be carried out.

Periodic safety reviews serve not only the confirmation of an existing safety level but should also plan measures to increase the safety level, if necessary.

In countries where the operation time of a nuclear power plant is limited by the permit, decisions are made on a long-term operation after the authorized term has expired, which is generally 40 years.

The French LTO strategy is explained in the ASN Report of 2016 (ASN 2016): *"EDF wishes to extend the operating life of its reactors currently in service well beyond forty years, the service life posited at their initial design stage. In the future, this fleet would function alongside new EPR or equivalent type reactors, meeting considerably strengthened safety requirements. The continued operation of the current reactors beyond forty years must therefore be examined taking account of the existence of safer technology. There are then two objectives. The licensee must first of all demonstrate the compliance of the reactors with the applicable regulations, more specifically by analysing and processing the problems of equipment ageing and obsolescence. It must also improve their level of safety with respect to the requirements applicable to the new reactors."*

Accordingly, approval to an LTO is possible only on the basis of a verifiable significant increase in the safety level. At the same time, the safety level set for new plants should be achieved as far as possible.

In accordance with the French explanations, therefore, it is to be required that in the case of NPPs with 900 MW reactors, after the *"4th safety review cycle of the periodic safety review, i.e. after 40 years of operation, a safety level corresponding to the safety status of the EPR will be achieved."* (ASN 2013)

At the same time, it must be demonstrated that the safety for the duration of the intended extension of the operating time remains in accordance with the applicable standards. The verification of the safety of non-changeable components and systems taking into account their aging is of particular importance.

This corresponds with previous announcements by ASN that the safety requirements for new nuclear power plants (EPR) should also be applied to existing nuclear power plants. It calls for:

"The safety objectives set by ASN for new nuclear reactors, such as EPR, accounted for the lessons learnt from the Three Mile Island accident in 1979 and the Chernobyl disaster in 1986, events which showed that severe accidents are not just a theoretical hypothesis.

These safety goals include, in particular with respect to reactors in operation:

- *Reducing the risk of accidents that may result in core meltdown*
- *In case of core meltdown, reducing radioactive releases to the environment, leading in particular to the presence of a corium catcher in the EPR.*

Following the events of September 11, 2001, the objective of resistance to large aircraft crashes has been strengthened." (ASN 2007)

ASN (2007) continues by stating: *„It is obvious that we expect more ambitious safety requirements for the EPR reactor as compared to the previous reactor generation. I can specify it in a more direct manner: we would not allow the construction of a N4 reactor anymore."*

The requirements for an operation over a period of 40 years must be compared to this statement. This announcement was made before the Fukushima accident, the high importance of external hazards on the safety of nuclear power plants was not considered.

The statement that in France in 2010 no N4-type plant would have been approved, of course, has an impact on a possible permit for the continued operation of the much older 900 MW plants beyond the original 40-year operating life

The prerequisite for operation of the 900 MW systems beyond the operating time of 40 years is proof of a safety level equivalent to that of the EPR.

Proof of safety must not be performed at the expense of the required design safety margins respectively

Of importance for the operation of the nuclear power plants in France is the implementation of any required retrofits within the framework of the 10-year PSR in order to achieve the required safety targets in (ASN 2016) in corresponding time limits. In any case, all required retrofitting must be carried out. (WENRA 2017).

Article 8a of the COUNCIL DIRECTIVE 2014/87 / EURATOM of 8 July 2014 (EU 2014) states:

"1. Member States shall ensure that the national nuclear safety framework requires that nuclear installations are designed, sited, constructed, commissioned, operated and decommissioned with the objective of preventing accidents and, should an accident occur, 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 radioactive 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 licence is granted for the first time after 14 August 2014;
   (b) is used as a reference for the timely implementation of reasonably practicable safety improvements to existing nuclear installations, including in the framework of the periodic safety reviews as defined in Article 8c(b)."

5.2 Results

- In the case of an LTO for nuclear power plants with 900 MW reactors after the 4th safety review of the periodic safety review, i. e. after 40 years of operation, , a safety level close to the EPR has to be reached.
- Any retrofitting deemed necessary to achieve this objective shall be performed prior to recommissioning of the plant after the 4th safety review.[70] Non-compliance with these requirements increases the risk of core meltdown accidents.
- The "timely implementation of reasonably practicable safety improvements" approach discussed in (WENRA 2017) only applies to necessary retrofits resulting from insights from the PSR during the 40-year operational period. This approach does not apply to the operation beyond this period. Approval to operation beyond the projected lifetime should be comply with the standards for the authorization of a new installation.

[70] ASN considers that EDF's work program must be built with the goal that all reactors of 900 MWe and 1300 which operate beyond the fourth safety review would be considered to have been the work and modifications required no later than the end of their fourth year inspection. /ASN 2013/

6 UPGRADE INTEGRATION COMPLIANCE

6.1 General Compliance Requirements regarding status and upgrade of plant

Given certain evidence from documentation of systems regarding manufacturing conditions and quality assurance as well as operation history and the accumulated loads, compliance cannot be demonstrated to the full extent against original certification.

Detailed reassessment of documentation and inspection and testing of physical structures, systems and components (SSCs) was intensified over the last years, also to prepare a consistent basis for the upcoming 4th Periodic Safety Review.

Documentation reassessment and inspections showed systematic quality deviations and methodological deficiencies also regarding systems relevant for safety.

The overview of selected Issues of Importance related to the broader aspects of them deteriorating is to be considered depending on Defense in Depth (DiD) provisions during accident scenarios. Systematic and comprehensive harmonization is a prime scoping requirement for the integration of improvements.

The origins of Initiating Events causing such widespread environmental impacts as a result from accidents must be considered in general consequences of successive deterioration and loss of Defense in Depth options.

Therefore the Defense in Depth provisions, respectively the elements of the DiD Concept(s) have to be examined for their availability, functionality, applicability and robustness.

The sequence of VD4 programs to be implemented and executed for the individual units of interest to this study must be checked for addressing the eventual DiD concerns and the safety enhancements and/or plant modifications as well.

Identification of non-compliance regarding manufacturing and operation documentation and verifiable physical status of SSCs, including comparison with established modelling of critical conditions and processes, also of the impacts of ageing is a precondition for a possible LTO beyond the original design lifetime and should be strictly required by ASN.

Compliance Status of the PWR 900 MWe fleet

The plants' operation history has provided extensive knowledge to suggest or even urge the implementation of plant modifications, improvements and changes as well; also experiences made at other plants, in particular in relevance to the questions raised and to major events that occurred in other NPPs during the operational life of the AP 900 plants.

The operator EDF should record the history and status of the compliance of SSCs in systematic and verifiable manner to full extent. Non-compliance issues, including missing compliance justification for safety critical systems, should be evaluated considering suspension of the operation license in distinct cases with immediate effect.

All compliance inconsistencies have to be clarified and resolved before a new license beyond 40 years for LTO can be issued, which should be established as a concept already in the generic phase.

The aim is to obtain indications about the DiD implications, resulting from issues identified and reported and help with:

- Non-conformities practical elimination;
- Manufacturing irregularities, counterfeit, fraudulent and suspect items;
- Corrective action requirements;
- Measures regarding Codes, Rules, Regulations and compliance.

This serves to define the safety level that is achieved through the implementation of the selected maintenance approaches. Issues to treat with regard to multiple units on one site are considered important and the associated safety considerations and resultant concepts as well.

Station Black Out sequences could be triggered by grid collapse. Forecasts warn of an inevitably increasing grid failure rate and such events could easily induce drastic nuclear island collective failures in combination with simultaneous SBOs of more than 1 unit .

Nuclear Power Plant Sites featuring multiple units, the setting for most French NPPs, are considered to experience in extended cases of unit Black Out situations multiple SBOs at these sites. Common Cause/Mode extended Nuclear Island Fallback Events, which would be prone to a total loss of offsite power.

The arising situation involves an augmented likelihood of sequences of SBOs. Under these circumstances the success of almost simultaneous actuation of the EPS is essential for the emergency situation management options.

Multiple units have a real thread potential not only when power output coast down sequences of the turbo-generators cause a fallback to nuclear island op-eration. With energy supply still needed, at least to provide for the cool–down capacity, reconfiguring the power supplies to the grid can be delayed. But the production could even fall short over extended time periods.

For longer periods of standby or shutdown operation cooling provisions can be needed.

As a consequence, increase on-site storage of diesel fuel is planned also, because net-recovery is likely to consume more time than originally expected at the time of the plants design verification and licensing.

The feasibility to add these additional power supply means within short intervention time periods and the options to connect them to coolant pumps for the cores as well as Spent Fuel Storage Pools (SFPs) should enhance considerably the mitigation options due to the possibilities for short intervention actions.

ASN Requirements to establish DiD as the systematic concept, that includes backfitting actions

Already at a generic level ASN should therefore set up detailed requirements on how AP 900 units can enhance compliance with the DiD concept on all levels. Fulfillment of the following criteria should be requested at least for:

- Demonstration of system status regarding all DiD levels considering redundancy, physical and functional separation of safety functions;

- Systematic lists of deficiencies regarding the existing systems;
- Gap analysis referring to a state-of-art DiD concepts;
- Proposal for back fitting actions for the AP 900 fleet associated with the respective DiD levels;
- Time frame and project implementation descriptions;
- Inspection and verification mechanisms.

Implementation of all measures should take place before an operation license is granted after completion of VD4s because the general DiD requirements and the plant safety concepts are well known for a longer time and preparation work appears to progress significantly.

Exemplary non Compliances Reported

Conformity Deviation in an emergency system, concerning valves electrical servomotors in the intermediate cooling loops 71

In response to a request by ASN the IRSN has assessed the impact on safety caused by the refusal of closure of 4 valves in the circuit ICL (RRI) of units 3 and 4 at the NPP Blayais in 2016 and 2017 respectively.

The cooling of safety relevant auxiliary systems as well as reactor protection systems is operated using motor actuated valves of this type. With the reactor in operation, the valves are in open position. In a confinement isolation situation the valves are supposed to close to prevent radioactive effluents passing. In case of an incident, the inability to close impairs the proper closure of the confinement. The delay caused by manually closing the valves outside containment – as the appropriate corrective action – and the possibility to even cause radioactive spill. Outside the confinement are even more valves of similar type, the control elements of many circuits which are also safety-relevant. Therefore the safety concern is generic.

In the past, EDF has determined a failure frequency of 5,2.10-4. Ever since the occurrences of this kind appeared rather frequently in various contexts, they were always traced back to the motors of the valves.

- Reasons and handling of the operability refusals
- Principal causes have been identified:
- A weak uncoupling of the manual coupling mechanism
- An inappropriate control by the limiter of the actuation
- A too low control-command response on actuation

In 2009 the lack of functionality was evident from several cases observed.

Lubrication was found to be insufficient. The grease lubricant was changed in 2012, and is supposed to last for 30 years[72]. The national maintenance procedures (Procédures Nationales de Maintenance (PNM)) suggest the use of grease in non-determined quantities. The user/supplier determines the sufficiency of the lubricant.

Ageing of the repositioning spring was also considered and other causes as well.

[71] Avis IRSN/2019-00025: Case concerning: All NPP vintages

[72] WENRA Safety Level for Existing Reactors, Issue I: Safety Area: Operation, September 2014

IRSN considers the two methods proposed by EDF adequate.

The lack of preventive maintenance planning in this context has been recognized and IRSN calls upon EDF to continue EDF-wide introduction.

A nationwide change of maintenance procedures respecting the recurrent lubrication grease notation of the quantities and locations within 6 month. Conformity checks at the next outage and partial the associated review activities. Also, as a temporary fix of the problem the adding of an active sealing device can be applied.

The limit switches should also be adjusted properly and functional repeatability checked as well as the electrical contacts.

For specific types of the servomotors an additional weight to counter the reset spring force or the application of a special closing device would be choices.

Replacement of the fire detection system at the Bugey NPP vintage CP0[73]

The exemplary statement reiterated by IRSN v/s EDF, related to requirements dating back to 2014, when a request was made by IRSN for the replacement of the fire detection system at the Bugey NPP[74]. It treated a number of non-conformities and inconsistencies[75].

Safety relevant Recommendations, 4 specific to the Bugey NPP vintage CP0

The noncompliance issues are related to the need for a complete refurbishment of the fire detection and fire alarm system at the NPP Bugey. There are significant shortcomings in these areas.

The related recommendation is also subject of recommendation #4 in the text source of this brief note.

Scoping and Refurbishing needs are as follows:

- Improve the reliability and performances of the fire detection system
- Treat obsolescence of the existing detection system
- Abolish the use of ionization detectors in compliance with the regulation
- Consequences resulting from un-availability of one or more fire centrals
- Classification and environmental service conditions of the detectors
- Impact on the modification of the Safety Report (RDS)
- Impact of the modifications on Chapter 9 of the RGE

The installation work will be done – depending on the locations within the units – in close coordination with other refurbishments. Similar work is also planned for the later vintages P4 and N4. In consequence the IRSN has issued a recommendation to Bugey NPP to also introduce a similar fire detection concept as in the N4 vintage plants.

The installation of cameras for fire detection is viewed as an addition with ambiguous merits, this is endorsed by experience at unit 2 of the Penly NPP in 2012.

---

[73] Avis IRSN N° 2016-00088: EDF, March 22, 2016: Case Citation

[74] https://www.grs.de/sites/default/files/pdf/grs-a-3845_0.pdf

[75] IAEA-TECDOC-1421 Experience gained from Fires in Nuclear Power Plants: Lessons learned, November 2004

IRSN recommend EDF to justify that fire surveillance in the GMPP bunker allows to define quickly adapted intervention dispositions and for straight fighting in case of fire in those bunkers.

IRSN recommend EDF to accomplish periodic checks of the fire detection system for the operation terminal JTD 001 HK located at the fire station JTD 001 AR of the NPP Bugey.

IRSN recommend EDF to accomplish periodic checks of the fire detection system for the area Pump Hall CRF of the units 4 and 5 connected to one of the Fire Centrals system JDT class IPS-NC.

IRSN recommend EDF to accomplish periodic checks of the fire detection system for the related TAC locations within the Bugey NPP.

6.1.1.1 Lifetime Extension – Safety upgrade ISSUES

For these plants of earlier designs the legal provisions in France require EDF to carry out safety reviews, periodically recurrent after 10 years of operation, these intended to follow up on changes over the plants' life, the particular objectives of which are to:

- Assess the facility's condition and its compliance with current regulations, as an integral part reviewing compliance and ageing management.
- Reassess the hazards and/or potential environmental damage resulting from plant operation and affecting nature, public safety, health and the environment, which are identified by legislation as Protected Interests.
- Scope is to make use of the assessment results in order to continuously improve performance in protecting the said interests.

Examplary safety upgrade issues

Steam Generator Integrity Issue(s)

The tubes are prone to outside diameter stress corrosion cracking at tube support plates. This became one of the dominating ageing mechanisms in steam generator tubes made of Inconel.

A variety of maintenance approaches were developed and implemented worldwide to enable safe and reliable plant operation with the affected tubes. Despite different philosophical and physical backgrounds involved, all applied approaches satisfy relevant regulatory requirements.

The main goal followed in the paper is to quantify the degree of safety, which is achieved through the implementation of selected maintenance approaches.

A method is proposed which measures the operational safety and availability through three efficiency parameters:

- Probability of steam generator tube rupture;
- Predicted accidental leak rates through the defects in the tube bundle;
- Number of plugged tubes.

In case of failures, leaks and subsequent rupture, the event initiations are imminent.

Severe Accident Management and Mitigation Provisions

A selection of Code Requirements related to the containments retention functions[76]:

F4.8 Isolation of the containment shall be possible in DEC. For those shutdown states where this cannot be achieved in due time, severe core damage shall be prevented with a high degree of confidence.

If an event leads to bypass of the containment, severe core damage shall be prevented with a high degree of confidence.

F4.9 Pressure and temperature in the containment shall be managed.

F4.10 The threats due to combustible gases shall be managed.

F4.11 The containment shall be protected from overpressure.

If venting is to be used for managing the containment pressure, adequate filtration shall be provided.

F4.12 High pressure core melt scenarios shall be prevented.

SSCs including their support functions and related instrumentation.

It is acknowledged that in case of DEC B, sub-criticality might not be guaranteed during core degradation and later on during some time in a fraction of the corium as well.

F4.13 Containment degradation by molten fuel shall be prevented or mitigated as far as reasonably practicable.

F4.14 In DEC A, radioactive releases shall be minimized as far as reasonably practicable.

In DEC B, any radioactive release into the environment shall be limited in time and magnitude as far as reasonably practicable to:

(a) Allow sufficient time for protective actions (if any) in the vicinity of the plant; and

(b) Avoid contamination of large areas in the long term.

Instrumentation and control for the management of DEC:

F4.15 Adequately qualified instrumentation shall be available for DEC for determining the status of plant (including spent fuel storage) and safety functions as far as required for making decisions.

F4.16 There shall be an operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations

ASN functions required regarding safety upgrades under LTO conditions

The list of examples provides an overview about a selection of safety upgrades with special relevance for the interest Austria advocates regarding prevention of

[76] WENRA Safety Level for Existing Reactors, Issue G: Design Basis Envelope for Existing Reactors, Safety Classification of Structures, Systems and Components, Containment Functions F 4.8 ff. 4.16, September 2014

any accident and obviously the mitigation of consequences.

ASN established, based on the legal framework, certain obligations to be fulfilled by the operator. The obligations are based on technical and methodological criteria.

Nevertheless it was demonstrated in the past, that even if back-fitting actions were requested by ASN, implementation on plant level were followed frequently with less persistence than estimated originally, significant deviations occurred due to different reasons.

Documentation on systematic and continuously applied upgrade programs beyond physical ageing management seems to be unavailable to the necessary extent for the public interested.

ASN is asked therefore to:

- Provide access to the criteria to qualify safety upgrades intended, including justification and verification methodologies
- Publish upgrade requirements on the generic (later on also on plant) vintage level, describing technical plant modifications in sufficient detail
- Set up a resilient time schedule for upgrade implementations
- Demonstrate and publish the certification and licensing of the features implemented, including deviation reports and corrective actions requirements and implementation schedules.

6.2 Results

Prerequisites for a life extension of a 900 MW NPP of the French CP0/CPY generation:

- Proof of compliance with the required safety margins over the intended service life extension, especially for the components designed for a duration of only 40a (without the use of probabilistic analysis results).
- All retrofits considered necessary to meet the safety objective – adaptation to the safety features of the EPR – shall be performed before recommissioning after the 4th safety review, in particular:
  - Consistent separation of the operational and the safety-related functions of the affected systems.
  - Increasing the degree of redundancy of the safety systems, including the safety-relevant supply systems
  - Ensuring the independence of the individual redundancies of the safety systems, even with the respectively assigned safety-relevant supply systems.
  - Proof of event-control of events classified as PCC-2 (Reference transients), PCC-3 (Reference incidents) and PCC-4 (Reference accidents) in the EPR.
  - Increasing the (real) resistance of the safety-relevant facilities even against extreme (beyond design basis) external influences (earthquake, plane crash .....). The structural plant components are of particular importance here.

- Installation of a complete safety level 4, in particular:
  - Complete installation of the "Hard Core" as a system of safety level 4a.
  - Proof of control of the plant conditions classified as RRC-A (Risk Reduction Category A) in the EPR.
  - Accident management measures shall also be available in the case of extreme external impacts. Their availability over a longer period is important.
  - Exclusion of cliff edge effects, even in the case of extreme external impacts.
  - Proof of the EPR's RRC-B (Risk Reduction Category B) classification of core meltdown phenomena with regard to limiting the release of radioactive material into the environment – level of defense 4b.

7 LITERATURE

Accident without core melt

ASN (2011): Complementary Safety Assessment of the French Nu-clear Power Plants. Report by the French Nuclear Safety Authority (December 2011).

ASN (2012a): Avis no2012-AV-0139 de l'Autorité de sûreté nucléaire du 3 janvier 2012 sur les évaluations complémentaires de la sûreté des installations nucléaires prioritaires au regard de l'accident survenu à la centrale nucléaire de Fukushima Daiichi.

ASN (2012b): National Action Plan of the French Nuclear Safety Authority. Complementary Safety Assessment Follow-up to the French Nuclear Power Plants Stress Tests.

ASN (2014a): Technical Guidelines for the design and construction of the next generation of Nuclear Power Plants with pressurized water reactors, 2014.

ASN (2014b): Updated National Action Plan of the French Nuclear Safety Authority. Follow-up to the French Nuclear Power Plant Stress Test (December 2014).

ASN (2016): Seventh National Report for the 2017 Review Meeting. Convention on Nuclear Safety.

ASN (2017): Update of the Action Plan of the French Nuclear Safety Authority, December 2017.

ASN (2018): Letter from ASN to EDF, Object : Réacteurs électronucléaires – EDF, Note de réponse aux objectifs du quatrième réexamen périodique des réacteurs de 900 MWe, 28. Septembre 2018.

ASN (2019a): Décision n° 2019-DC-0662 de l'Autorité de Sûreté Nucléaire du 19 février 2019 modifiant les décisions n° 2012-DC-0274 à n° 2012-DC-0283, n° 2012-DC-0285 à n° 2012-DC-0290 et n° 2012-DC-0292 du 26 juin 2012 fixant à Électricité de France – Société Anonyme (EDF-SA) des prescriptions complémentaires applicables aux sites électronucléaires de Belleville-sur-Loire, Blayais, Bugey, Cattenom, Chinon, Chooz B, Civaux, Cruas-Meysse, Dampierre-en-Burly, Flamanville, Golfech, Gravelines, Nogent-sur-Seine, Paluel, Penly, Saint-Alban et Tricastin au vu des conclusions des évaluations complémentaires de sûreté (ECS).

ASN (2019b): ASN, Note d'information, Centrale nucléaire de Fessenheim: l'ASN modifie certaines de ses prescriptions compte tenu de l'arrêt définitif prévu de la centrale, Publié le 27/02/2019.

EU (2014): Council Directive 2014/87/EURATOM of 8 July 2014.

FERRARO, G. (2015, February): EDF France modernization program for the existing NPPs. OECD/NEA Workshop Innovations in Water-cooled Reactor Technologies, Paris.

IAEA (1999): Anticipated Transients Without Scram For Wwer Reactors Iaea, Vienna, 1999, IAEA-EBP-WWER-12.

IAEA (2006): Fundamental Safety Principles, No. SF-1, IAEA 2006.

IAEA (2016): Safety of Nuclear Power Plants: Design (IAEA Safety Standards Series - Specific Safety Requirements SSR-2/1 (Rev. 1)), Vienna, Austria.

IRSN (2015a): IRSN, Nuclear Power Reactor, Core Melt Accidents, Current State of Knowledge, 2015.

IRSN (2015b): IRSN, Safety and Radiation Protection at Nuclear Power Plants in France in 2014, IRSN'S POSITION 2015.

IRSN (2015c): Didier Jacquemain et.al., Past and Future R&D at IRSN on Corium Progression and Related Mitigation Strategies in a Severe Accident, NURETH-16, Chicago, IL, August 30-September 4, 2015.

IRSN (2016): IRSN, Safety and Radiation Protection at Nuclear Power Plants in France in 2015, IRSN'S POSITION 2016.

IRSN (2018): Concertation À L'occasion Du 4ème Réexamen Périodique Des Réacteurs De 900 Mwe Du Parc Électronucléaire Français - Foire Aux Questions, IRSN Octobre 2018.

IRSN (2018a): IRSN, Master of aging under fourth-year inspections of the 900 MWe reactors, February 23, 2018.

OECD (2015): Questionnaire on Long-Term Operation of Commercial Nuclear Power Plants Nuclear Safety NEA/CSNI/R(2015)13, July 2015.

WENRA (2013): WENRA, Report Safety of new NPP designs, March 2013.

WENRA (2014): WENRA Safety Reference Levels for Existing Reactors, September 2014.

Internal/external hazards

ASN (1980): ASN, RFS-I.2.a. du 05/08/1980, Prise en compte des risques liés aux chutes d'avions.

ASN (2001): ASN, Basic Safety Rule, Fundamental safety rule n°2001-01 concerning basic nuclear installations.

ASN (2001a): Protection des installations nucléares contre les chutes d'avions, ASN 13/09/2001.

ASN (2012): ENSREG, National Action Plan of the French Nuclear Safety Authority, December 2012.

ASN (2013): Protection of Basic Nuclear Installations Against External Flooding, ASN GUIDE N° 13 Version of 08/01/2013.

ASN (2014a): "Technical Guidelines for the design and construction of the next generation of nuclear pressurized water plant units", ASN 2014.

ASN (2014b): Updated National Action Plan of the French Nuclear Safety Authority. Follow-up to the French Nuclear Power Plant Stress Test. Autorité de Sûreté Nucléaire (ASN) (December 2014).

ASN (2015): ASN – Letter to EdF Nuclear Operation Division, Montrouge 20. March 2015.

ASN (2016): Seventh National Report for the 2017 Review Meeting. Convention on Nuclear Safety.

ASN (2016a): ASN position statement of 20th April 2016 concerning generic guidelines for the periodic safety review associated with the fourth ten-year inspections for the 900 MWe reactors, Published on 21/04/2016.

ASN (2017): Guide de l'ASN n°22 : Conception des réacteurs à eau sous pression, Publié le 18/07/2017.

ASN (2017a): ASN, Olivier GUPTA, Nuclear Safety in France Upcoming challenges, EUROSAFE 2017.

ASN (2017b): Updated National Action Plan of the French Nuclear Safety Authority.

ASN (2017c): Questions Posted To France in 2017. Convention on Nuclear Safety.

ASN (2018): ASN report on the state of nuclear safety and radiation protection in France in 2017, ASN 2018.

BERGE (2014): BERGE-THIERRY Catherine: Seismic Hazard Assessment and Uncertainties Treatment: Discussion on the current French regulation, practices and open issues, NEA/CSNI/R(2014)9.

BERGE (2016): Catherine BERGE-THIERRY: Nuclear Safety & Seismic Risk Management In France: Overview, September 28, 2016, Scientific & Technical Seminar At The Canadian Nuclear Safety Commission.

CNS (2014): Convention on Nuclear Safety, Questions Posted To France in 2014.

EDF (2011): Rapport d'évaluation complémentaire de la sûreté des installations nucléaires au regard de l'accident de Fukushima.

EUR (2012): European Utility Requirements for LWR NPPs (2012), Revision D.

EUROSAFE (2015): French Post-Fukushima Complementary Assessments, EUROSAFE 2015.

FANC (2015): Class I Guidances, Guideline on the categorization and assessment of accidental aircraft crashes in the design of new class I nuclear installations, FANC, February 2015.

FERRARO (2015): Ferraro, G., EDF France modernization program for the existing NPPs. OECD/NEA Workshop Innovations in Water-cooled Reactor Technologies, Paris.

FLAB (1984): Methodology for coping with accidents of external and internal origin in PWR power stations, EUR 10782 EN, August 1984.

IAEA (2006): Safety of Nuclear Power Plants: Design (IAEA Safety Standards Series - Specific Safety Requirements SSR-2/1 (Rev. 1)), Vienna, Austria.

IAEA (2010a): Seismic Hazards In Site Evaluation For Nuclear Installations, Iaea Specific Safety Guide SSG-9, Vienna 2010.

IAEA (2010b): Meteorological And Hydrological Hazards In Site Evaluation For Nuclear Installations, Iaea Specific Safety Guide SSG-18, Vienna 2010.

IAEA (2012): Safety Requirements In France For The Protection Against Extreme Earthquakes, International Experts Meeting on Protection against Extreme Earthquakes and Tsunamis, IEM3 IAEA, Sept. 2012.

IAEA (2016): Site Evaluation for Nuclear Installations (IAEA Safety Standards Series - Safety Requirements NS-R-3 (Rev. 1)), Vienna, Austria , 2016.

IRSN (1996): Libman, Elements of nuclear Safety, IRSN, 1996.

IRSN (2015a): IRSN, Temporary and Long Term Design Provisions Taken on the French NPP Fleet to Cope with Extended Station Black out in case of Rare and Severe External Events, NEA/CSNI/R(2015)4.

IRSN (2014): IRSN, O. Scotti, C. Clément and D. Baumont, Seismic hazard for design and verification of nuclear installations in France: regulatory context, debated issues and ongoing developments, Bollettino di Geofisica Teorica ed Applicata Vol. 55, n. 1, pp. 135-148; March 2014.

IRSN (2014a): IRSN'S POSITION, Safety and Radiation Protection at Nuclear Power Plants in France in 2014 IRSN 2015.

ORDER (2012): Order of 7 February 2012 setting the general rules relative to basic nuclear installations, JORF (Official Journal of the French Republic) No. 0033 of 8 February 2012, page 2231.

SMIRT (2015): Aybars Gürpinar, Antonio R. Godoy, James J. Johnson, Considerations For Beyond Design Basis External Hazards In Npp Safety Analysis, SMiRT-23, Manchester, United Kingdom - August 10-14, 2015 Division IV, Paper ID 424.

U.S. Reg. (1984): Stevenson; J.D.: Summary and Comparison of current U.S. Regulatory Standards and foreign Standards, Nuclear Engineering and Design (1984) 145-160.

WENRA (2014): WENRA Safety Reference Levels for Existing Reactors, September 2014.

WENRA (2015): WENRA Guidance Document Issue T: Natural Hazards, 21 April 2015.

Core melt accidents

ASAMPSA (2013): Advanced Safety Assessment Methodologies: Level 2 PSA Technical report ASAMPSA2/WP2&3/ 2013-35 Rapport IRSN/PSN-RES/SAG/2013-0177, 30/04/2013.

ENSREG (2012): Compilation of recommendations and suggestions. Peer review of stress tests performed on European nuclear power plants; 2012.

Spent fuel

ALVAREZ (2003): R. Alvarez et al.: Reducing the Hazards from Stored Power-Reactor Fuel in the United States, Science & Global Security, Vol. 11, No. 1 (2003).

BMU (2002): Schutz der deutschen Kernkraftwerke vor dem Hintergrund der terroristischen Anschläge in den USA vom 11. September 2001. Zusammenfassung de GRS-Studie durch das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU). Bonn, den 27.11.2002.

ENSREG (2012): Compilation of recommendations and suggestions. Peer review of stress tests performed on European nuclear power plants; 2012.

HIPPEL (2016): Reducing the Danger from Fires in Spent Fuel Pools; Frank N. von Hippel and Michael Schoeppner; SCIENCE & GLOBAL SECURITY 2016, Vol 24, No.3, 141-173; http://dx.doi.org/10.1080/08929882.2016.1235382

PETRANGELI (2010): Large airplane crash on a nuclear plant: Design study against excessive shaking of components; G. Petrangeli; Nuclear Engineering and Design 240 (2010), p. 4037-4042.

Implementation of necessary upgrades in time

ASN (2010): Statement of ASN Commission: "Which level of safety for new nuclear reactors built around the world? ", Published on 07/07/2010.

ASN (2013): Lettre de suite, EDF proposed generic program for the continued operation of operating reactors beyond their fourth safety review, Montrouge, June 28, 2013.

ASN (2016): The ASN (Nuclear Safety Authority) Report on the state of nuclear safety and radiation protection in France in 2015, March 2016.

EU (2014): Council Directive 2014/87/EURATOM of 8 July 2014 amending Directive 2009/71/Euratom establishing a Community framework for the nuclear safety of nuclear installations.

WENRA (2017): WENRA Guidance Article 8a of the EU Nuclear Safety Directive: “Timely Implementation of Reasonably Practicable Safety Improvements to Existing Nuclear Power Plants”, 2017.

ENVIRONMENT AGENCY AUSTRIA **umweltbundesamt**

Umweltbundesamt GmbH
Spittelauer Lände 5
1090 Vienna/Austria

Tel.: +43-(0)1-313 04
Fax: +43-(0)1-313 04/5400

office@umweltbundesamt.at
www.umweltbundesamt.at

EMAS
Geprüftes Umweltmanagement
REG.NO. AT- 000484

ISBN 978-3-99004-505-3