Health and Safety Executive

# IAEA Generic Review for UK HSE of New Reactor Designs against IAEA Safety Standards
# EPR

# IAEA Generic Review for UK HSE of New Reactor Designs against IAEA Safety Standards
# EPR

## 3.1–3.7 Graded Approach

### 3.2–3.3

**3.2 A graded approach shall be used in determining the scope, extent, level of detail and effort that needs to be devoted to the safety assessment carried out for any particular facility or activity.**

**3.3 The main factor taken into consideration in the application of a graded approach to the safety assessment shall be the magnitude of the potential radiation risks arising from the facility or activity. This needs to take into account any releases of radioactive material in normal operation, the potential consequences of anticipated operational occurrences and accidents, and the possibility of occurrence of very low probability events with potentially high consequences**

Review Results

The Requirement is addressed. The scope, extent, level of detail and effort is consistent with the potential of a nuclear reactor for core degradation accidents with large radioactive releases. Safety analyses have been performed in order to determine whether the design and engineered safety features fulfil the safety functions required of them.

Detailed information is provided on how regulatory requirements are met. Each Chapter of the Design and Safety Report is preceded by the related Technical Guidelines (TGs), i.e. the requirements of the French regulator, which are addressed. Chapter H provides information on the licensing reviews by the French and the Finnish Regulator and a comparison to the WENRA reference levels.

Results of accident analyses are provided in Volume 2 Chapter P 'Reference Operating Condition Studies'. Considering six categories of plant operational states the Design Basis Events are grouped into four Plant Condition States (PCCs) based on their estimated frequency and impact.

Both deterministic and probabilistic analyses are performed with the objective to demonstrate that an adequate level of safety has been achieved. At this stage a Level 1+ PSA is available only and is briefly summarized in Volume 2 Chapter R. It is stated that since the design of the EPR is not yet finalized the "Level 2 PSA model remains evolutionary".

The possibility of occurrence of very low probability events with potentially high consequences is taken into account. In particular, design features are included, which respond to the IAEA NS-R-1 Requirement that "in addition to the design basis, the performance of the plant in specific accidents beyond the design basis, including selected severe accidents, shall also be addressed in the design". Special features are aimed at preventing high pressure core melt accidents and to protect the containment integrity in case of low pressure severe accidents by arresting a molten core within a core retention system below the PRV.

**3.4 A graded approach to safety assessment shall also take into account other relevant factors such as the maturity or complexity of the facility or activity. The maturity relates to the use of proven practices and procedures, proven designs, data on operational performance of similar facilities or activities, uncertainties in the performance of the facility or activity, and the availability of experienced manufacturers and constructors. The complexity relates to the extent and difficulty of the effort required to construct a facility or implement an activity, the number of the related processes for which control is necessary, the extent to which radioactive material has to be handled, the longevity of the radioactive material, the reliability and complexity of systems and components and their accessibility for maintenance inspection, testing and repair.**

Review Results

The Requirement is addressed. The safety assessment makes reference to the maturity of the design by documenting the long process, including international participation, of developing the Technical Guidelines for the design of the EPR. It is mainly based on the extensive experience with the operation of French and German PWRs.

Safety assessments are presented for the innovative features. Reference is made to related experiments and analyses as documented in an extensive list of publications including many references to experimental results from test facilities. This information could not be reviewed at this stage and has to be reviewed at the next step.

Volume 2 subchapter R.3 provides information on the use of PSA to consolidate the list of multiple failure conditions (RRC-A) to be addressed in the design by additional measures. Chapter S “Risk Reduction Categories” describes measures to address RRC-A and RRC-B (core melt) failure conditions.

## 3.5–3.6

**3.5 At the start of the safety assessment, a judgement shall be made on the scope, extent, level of detail and the effort that needs to be applied to the safety assessment for the facility or activity.**

**3.6 The application of the graded approach shall be reassessed as the safety assessment progresses and a better understanding is obtained of the potential radiation risks arising from the facility or activity. The scope, extent and level of detail of the safety assessment and the effort applied shall be adjusted accordingly.**

Review Results

The Requirement is addressed by responding to the Requirements for safety assessment for NPPs as specified in NS-R-1. At this stage a Preliminary Safety Report only had been requested. However, the Head Document is accompanied by a detailed ‘Design and Safety Report’ commensurate with the potential radiation risk arising from an NPP.

# 4.1–4.15 Overall Requirements

**4.3 The primary purpose of a safety assessment shall be to determine whether an adequate level of safety has been achieved for a facility or activity and whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body, reflecting the radiation protection requirements as established in the Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources [4], have been complied with. This includes the requirements in respect of radiation exposure of workers and the public, and any other requirements to help ensure the safety of facilities and activities.**

Review Results

The Requirement is addressed as documented in the Fundamental Safety Overview Document. The summary "Head Document" (Volume 1) follows the structure of the UK HSE request and gives guidance on where more detailed information is presented in the "Design and Safety Report" (Volume 2) and the "Environmental Impact Report" (Volume 3). Volume 2 is based on the publicly available parts of the French Preliminary Safety Report for the Flamanville-3 EPR. Volume 3 is based on the Environmental Assessment for the Flamanville-3 EPR. The EPR has been developed to meet the EPR Technical Guidelines (TGs) established by the French Nuclear Regulatory Agency (DGNSR) as requirements. For easy reference the chapters of the Design and Safety Report are preceded by the relevant requirements which apply. It is stated in Volume 1 Chapter C that the "TGs are deterministic in nature and no requirements are stated to estimate individual risk, or to demonstrate that risks are ALARP, which mirror current UK practices". It is indicated in the report that the UK ALARP principles will be addressed in the Pre-Construction Safety Report, which will also include an extension of the present PSA Level 1+ to Level 2/3 PSA.

The report addresses radiation protection requirements for workers and the public for normal operation and accident conditions. The Design Basis Events are grouped into 4 Plant Condition States (PCCs) based on their estimated frequency and impact. The radiological acceptance criteria for the PCCs are listed in Chapter 5.2.2.1. Cross reference information is provided on how they relate to the fuel damage states used in the analyses. Detailed information on accident analyses is provided in Chapter P 'Reference Operating Condition Studies' of the Design and Safety Report. For the purpose of the analyses the operational states of the reactor are grouped into 6 categories.

Results of the PSA Level 1+ are briefly summarized in Chapter R. The chapter includes the probabilistic design targets used for the EPR. Reference is made to differences in the use of targets and objectives not to be interpreted as design limits.

Subchapter R.3 provides information on the use of PSA to consolidate the list of multiple failure conditions (RRC-A) to be addressed in the design by additional measures. Chapter S 'Risk Reduction Categories' describes measures to address RRC-A and RRC-B (core melt) failure conditions.

Chapter H of the Head Document provides information on the licensing reviews by the French Regulator and the Finnish Regulator. The preliminary review by the US NRC is expected to lead to a formal application for design certification to be submitted late in 2007.

Results of an assessment against WENRA reference levels are reported. A comparison to the EURs will be updated. It can be inferred that the IAEA Requirements are addressed.

The EPR TGs are in principle deterministic and thus more information has to be provided in the next step on how the UK HSE SAPs will be met. This will include providing a Level 2 and 3 PSA as is planned for in the report. The use of probabilistic targets vs. objectives and design limits will have to be addressed.

The selection of the RRC-A and B list of failure conditions addresses IAEA Requirement NS-R-1 in the design “specified accidents beyond the design basis”.

It is noted that the Finnish regulator has requested additional design safety measures for the Okliluoto-3 EPR, which were not included in the UK design.

**4.4 The safety assessment shall include an assessment of the radiological protection provisions in place to determine whether the radiological risks are being controlled within specified limits and whether they have been reduced to a level that is as low as reasonably achievable. This will also provide an input into applying the other principles as indicated in Section 2.**

Review Results

The Requirement is addressed. Information is provided on how occupational and public radiological risks are being controlled within the recommendations of ICRP 60, the Euratom Directive 96/29 from 1996 and the more stringent EPR basis of design (TGs).

The approach to estimate annual occupational radiation exposure is described in Volume 2 Chapter L. The results are compared to the applicable standards and the experience with modern NPPs in operation. Detailed assessments are reported on how the ALARA principle has been implemented.

The method for calculating public radiation exposure from normal operation is described in Volume 3, Chapter D. 7. The information provided is based on the environmental impact report for the Flamanville -3 EPR. Adjustments will be made regarding potential UK sites.

ALARP considerations for accidental occupational risk will be provided later in accordance with the UK HSE SAPs. Design measures have been implemented to address the ALARP principle related to public accidental risk.

It is indicated that additional calculations will be performed to specifically address the UK HSE SAPs.

**4.5 The safety assessment shall address all the radiation risks that arise from normal operation, anticipated operational occurrences and accident conditions. The safety assessment for anticipated operational occurrences and accident conditions shall also address the way in which failures might occur and the consequences of any such failures.**

Review Results

The Requirement is addressed. Information is provided for 6 standard operational states of the reactor. Chapter P of Volume 2 “Reference Operating Condition Studies” addresses the categories of design basis events included in the IAEA Requirements.

Chapter S of Volume 2 addresses the IAEA Requirement (NS R-1, 5.6) that “specified accidents beyond the design basis, including selected severe accidents, shall also be addressed in the design”. Two categories are addressed in the documentation. RRC-A sequences are addressed in Chapter S.1 and cover the multiple failure conditions that are not considered in the PCC analysis of Chapter P. The list of failure conditions addressed is based on the PSA results as reported in Chapter R.3. RRC-B sequences are accident situations with core melt that would lead to large early releases. According to the EPR design principles these must be “practically eliminated”. These RRC-B accident conditions are addressed in Chapter S.2.

A summary of the PSA Level 1+ is provided in volume 2 Chapter R. A Level 2/3 PSA will be provided in the next step.

Emphasis is given to the defence-in-depth approach. The analyses address the categories of normal operation and accidents as used in the IAEA Requirements. Information is provided on how beyond design basis accidents are addressed in the design. It is recognized that the TGs providing the basis for the EPR design are deterministic in principle.

The PSA will be extended to a Level 2/3 PSA in the next step. This will also include more detailed information on how the targets and limits of the UK HSE SAPs are met.

**4.9 The safety assessment shall identify all the safety measures necessary to control radiation risks. It shall be determined whether the design and engineered safety features fulfil the safety functions required of them. It shall also be determined whether adequate measures have been taken to prevent anticipated operational occurrences or accident conditions and whether the radiation risks would be mitigated should they occur.**

Review Results

The Requirement is addressed. The design is based on the EPR TGs which have been developed based in particular on the French and German experience with PWRs. Sub-chapter P.0 of Chapter P "Reference Operating Condition Studies" gives a list of the initiating events studied and the acceptance criteria used. The chapter then presents the result of the accident analyses to determine whether the design and engineered safety features fulfil the safety functions required of them. The analyses include events associated with the fuel storage pool. It is stated that the frequencies for anticipated operational occurrences and accidents have been reduced by improvement of the defence-in-depth concept at all levels. The design provides for increased redundancy and separation, improved man-machine interface and extended response time for operator action.

Chapter S describes features to prevent core damage from multiple failure conditions (RRC-A sequences), and features to mitigate low pressure core melt accidents or to "practically eliminate" high pressure core damage accidents (RRC-B sequences). This approach addresses the NS R-1 Requirement to address in the design specified accidents beyond the design basis, including selected severe accidents.

The concept of accident categories which have to be "practically eliminated" is included in the IAEA Safety Standards in a footnote. It is stated in NS-R-1 that PSA shall be used "to verify compliance with probabilistic targets, if set." However, no such targets are included in the Requirement itself. The supporting guide NS-G-1.2 'Safety Assessment and Verification' does not set any targets either, but makes reference to the targets proposed by INSAG. These include probabilistic targets for large radioactive releases (1.0 E-6 per reactor-year for future plants). As an alternative, the guide refers to the following statement by INSAG: "Another objective for these future plants is the practical elimination of accident sequences that could lead to large early release, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analysis so that their consequences would necessitate only protective measures limited in area and time." The IAEA Safety Standards further specify the term 'practical elimination' in NS-G-1.10 as "if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise".

This concept of 'practical elimination' referred to in the IAEA Safety Standards is an important feature of the EPR design. For demonstrating 'practical elimination' the EPR analyses make use of a probabilistic value of 1.0 E-7 complemented by additional deterministic analyses (Volume 2, R.0.5.3).

At this stage a Level 1 + PSA is used to obtain estimates on how probabilistic criteria are met.

**4.10 The safety assessment shall address the radiation risks arising from the facility or activity to all the individuals and population groups who might be affected. This shall include the local population and population groups that are geographically remote from the facility or activity giving rise to the radiation risks, including those in other States as appropriate.**

Review Results

The Requirement is addressed. The methods for calculating public radiation exposure from normal operation are described in Volume 3 Chapter D. 7. Detailed information is provided for individuals and population groups based on the environmental impact report for the Flamanville- 3 EPR. Design measures are aimed at reducing the radiological effects of a severe accident with core-melt to the level which will not necessitate population evacuation or any long-term restrictions in food production.

Detailed assessments have been performed for the Flamanville site. A re-evaluation will be made regarding potential UK sites.

**4.11 The safety assessment shall address the radiation risks now and in the future. This is particularly important for activities such as the long term management of radioactive waste where the effects could span many generations.**

Review Results

The Requirement is addressed. An evaluation of the radiation risks posed by the facility is given in Requirement 4.19. Efforts to minimize radioactive waste are briefly described in Volume 2 Chapter T. Novel design features have been added to the design with the aim of 'practically eliminating' large early releases with the potential for long-term effects. Information is provided regarding design measures to address the ALARP principle regarding public accidental risk.

**4.12 The safety assessment shall determine whether adequate defence-in-depth has been provided, as appropriate, through a combination of several layers of protection (i.e. physical barriers, systems to protect the barriers and administrative procedures), that would have to fail or be bypassed before harm could be caused to people or the environment.**

Review Results

The Requirement is addressed. At the outset of Volume 2 Chapter C "Design Basis and General Layout" it is stated that the safety approach at the design level is based on the concept of defence-in-depth. The 5 levels of defence-in-depth summarize the concept as contained in IAEA NS R-1. The combination of several layers of protection is present throughout the design. The design includes innovative measures (practically excluding high pressure core damage accidents, core melt retention system) to strengthen the $4^{th}$ level of defence thus reducing the need for measures at the $5^{th}$ level.

The basic approach to the safety of the EPR is deterministic based on the defence-in-depth concept. The approach is complemented by probabilistic analyses limited to a PSA Level 1+ at present. A level 2/3 PSA is planned for.

A more detailed assessment of the defence-in-depth provisions is given in Requirement 4.45 to 4.48.

**4.13 In most cases, the safety assessment includes a safety analysis, which consists of a set of different analyses for quantitatively evaluating and assessing challenges to safety under various operational states, anticipated operational occurrences and accident conditions, using deterministic and probabilistic methods as appropriate. The safety analysis shall be an integral part of the safety assessment.**

Review Results

The Requirement is addressed. The safety assessment includes the results of safety analyses for events grouped into the 4 categories corresponding to operational states, anticipated operational occurrences and accident conditions. The documentation in Volume 2, Chapter P includes a description of the results of the safety analyses performed for the different initiating events. However, no details in the form of diagrams of the thermal hydraulic analyses are provided. The basic approach to the safety assessment is deterministic as presented in Volume 2, Chapter P, Reference Operating Condition Studies, complemented by probabilistic analyses presented in Chapter R. The Level 1+ PSA will be extended to a Level 2/3 PSA. A special Chapter S ‘Risk Reduction Categories’ addresses risk reduction measures using best estimate rather than conservative analyses. Some analyses are waiting for a detailed final design of the systems. These are usually addressed by bounding considerations.

The use of best estimate analysis methodology is recommended in NS-R-1 for analysis of accidents beyond the design basis.

**4.14 The computer codes that are used to carry out the safety analysis shall be verified and validated and this shall form part of the supporting evidence presented in the documentation. As part of the management system, the operating organization and the regulatory body shall seek improvements to the tools and data that are used.**

Review Results

The Requirement is addressed. Though no comprehensive list of computer codes for accident analysis is included in Volume 2, Chapter P, they are referred to in the text or references. Regarding severe accident analysis the Volume 2, Chapter S.2.2 makes more detailed reference to the computer codes used (e.g. MAAP, COREFLOW). It also describes the experimental evidence by referring to the related national and international (e.g. NEA/OECD) studies and the related publications. Additional information is provided in 4.60.

A more systematic documentation of the computer codes used should be provided for the next review phase.

**4.15 The results of the safety assessment shall be used to identify appropriate safety related improvements to the design and operation of the facility or conduct of the activity. These results allow assessment of the safety significance of unremedied shortcomings or of planned modifications and may be used to determine their priority. They may also be used to provide the basis for continued operation of the facility or conduct of the activity.**

Review Results

The Requirement is addressed. Chapter C of the Head Document describes the long iterative process of French and German co-operation leading to the EPR design. Table 1 of Chapter H provides a list of IRSN review reports since April 1992. During the 15 year design period about 90 EPR design assessments reports were issued by IRSN. These reports were reviewed by the French Standing Group for Nuclear Reactors (GPR).This independent advisory body included scientists and engineers from France, other European countries and the USA.

A comparison of the main design parameters of the EPR in comparison to the N4 and the KONVOI reactors are given in Volume 2, Chapter B.3. Volume 2, Chapter R.3 demonstrates how in an iterative process the results of the PSA have been used to provide features aimed at preventing core damage resulting from multiple failure conditions.

## 4.19 Potential Radiation Risks

**4.19 The potential radiation risks[1] associated with the facility or activity shall be identified and assessed. This includes the radiation exposure of workers and the public and the release of radioactive material to the environment associated with anticipated operational occurrences or accidents that lead to a loss of control.**

Review Results

The Requirement is addressed. Radioactive sources in the primary circuit are defined in Chapter 2.L.2. The specific activities are explained in detail in Chapter K.1. In radiation protection, the following two source terms are used:

- operational source term data is used to calculate worker dose estimates and for defining the facility Pressurized Nuclear Equipment (ESPN) classification (see Chapter C.2),
- biological protection design basis source term is used as a design parameter for EPR buildings, systems and shielding provisions.

Surface deposited activity, which represents a major contributor to worker dose due to ionising radiation, is detailed in Section 2 within Subchapter L.2.

Specific concentrations of radionuclides in the primary circuit affecting radiation protection are determined in 2L2 Table 1 for normal operations, and in 2L2 Table 2 for shutdown transient. Corrosion products radioactive deposits in the primary loops (RCP 1, 2, 3, and 4) are shown in 2L2 Table 3.

The collective dose to workers resulting from normal operation of the EPR, especially from outage operations, is assessed as shown in Vol. 2 Ch. L.3 to be 0.37 man Sv/reactor-year. It is based on the assumption of a standard EPR workforce.

The impacts on the site are evaluated (3.E.9.3). Based on the experience of previous PWRs in France and extrapolating this experience on the basis of design measures implemented in the EPR, the effective annual dose to the persons of the public located in the vicinity of the plant is estimated as 1 µSv due to liquid and 3 µSv due to gaseous wastes (6 µSv for the specific case of babies). (1.F.6.2.)

Under design basis events conditions, the radiological consequences are defined in 1.F. Table 5-4.l.

For design basis transients (PCC2) the long term doses for adults at 2 km distance and for children the 7 days dose at 500 m from the reactor do not exceed 6.9 E-5 Sv and 2.5 E-5 Sv respectively; for design basis incidents (PCC3- e.g. SGTR) 1.2 E-4 Sv and 4 E-4 Sv respectively; and for design basis accidents 6.1E-4 and 5.5E-3, respectively. In the case of DBAs, the highest doses correspond to the accidents with containment bypass, namely fuel handling accidents and Steam Generator Tube Rupture.

[1] The term ‘potential radiation risks’ relates to the radiological consequences that would occur when no credit is taken for any of the safety systems or protective measures incorporated for the facility or activity.

In the case of severe accidents the total core melt frequency is found to be 6.1 E-7/ reactor-year, which is very low, and what is even more important, the contribution of sequences with containment bypass is reduced to 4.09E-9/ reactor-year. Since containment bypass sequences involve the highest radiation doses, and all other core melt sequences result in much smaller radiological consequences, this characteristic of the EPR is very important.

The sequences with large releases are divided into several Plant Damage States, of which the PDS 1- corresponds to total or partial core damage with EVU [CHRS] and available mitigation methods (hence no failure of containment), PDS 2 – to low pressure core damage with EVU [CHRS] unavailability (late failure of containment) and PDS 3 to core damage with potential early failure of containment.

Evaluation of the dose to workers resulting from normal operation of the EPR will be further refined in the future, in particular with the assessment of individual doses and the consideration of abnormal events.

The radiological hazards in case of design basis incidents and accidents are determined, including population doses at various distances from the reactor. However, in the case of severe accidents, only the frequency of various Plant Damage States is given. Although it can be understood that the doses in the case of PDS 1 are much smaller than in PDS 2, and the doses in PDS 2 are much less than in PDS 3, the range of values is not given. While the reduction of PDS 3 frequency is a significant achievement, it would be better understood if the comparatively smaller consequences of PDS 2 and PDS 1 were shown. It is proposed that in the next step the safety report should provide these values.

## 4.20–4.21 Safety Functions

**4.20 All safety functions associated with a facility or activity shall be identified and assessed. This shall include the safety functions associated with the engineered structures, systems and components, any physical or natural barriers and inherent safety features as applicable, and any human actions necessary to ensure the safety of the facility or activity. This is a key aspect of assessment and is vital to the assessment of the application of defence-in-depth (see pars. 4.45 to 4.48). An assessment shall be undertaken to determine whether the safety functions can be achieved for all normal operational modes (including start-up and shutdown where appropriate), all anticipated operational occurrences and the accident conditions that need to be taken into account.**

Review Results

The Requirement is addressed. The safety function 'Control of Reactivity' [Head Doc. Ch. F 3.2.3, DCD Ch.D5] covers operational occurrences up to accidents and start-up and shutdown sequences. The shutdown margins are such that the reactor can be made sub-critical from all design stages and maintained sub-critical; reactivity transients are controllable within acceptable limits [DCD Ch. D 3.1.6,]. A Remote Shutdown Station exists [DCD Vol.2 Ch.62 1.3.3].

The safety function 'Heat Removal from the Core' is carried out by 4 separated active systems powered by diesels. The safety function "Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases" is addressed and the release values are estimated to be well below required limits [Head Doc. 3.2, DCD Vol2. Ch.P.3, Ch.R1.3.2-4, R4.3] for internal events as well as for external hazards; special emphasis is given to containment penetrations [DCD Vol.2 Ch. C 5.2; DCD Ch. F.2.3]. The annulus between the inner and outer shell is kept on sub-atmospheric pressure.

Based on the three fundamental safety functions, the plant specific safety functions have been derived and are listed comprehensively in Vol. 2C2. This is the basis for the identification and classification of the SSCs, including the associated requirements. This covers the mechanical classification, functional classification, system classification, seismic classification, electrical equipment classification, I&C classification as well as structural classification. All classified systems and related classification requirements are set out in dedicated tables (C2 Tab 3 to 7).

The link with defence-in-depth is made through the application of technical directives (technical guidelines) for the design and construction of the next generation of pressurized water nuclear power plants. All operational modes are considered (including shutdown states) and the level of system or components is addressed.

**4.21 The assessment of the safety functions shall determine whether they will be carried out with an adequate level of reliability consistent with the graded approach (see Section 3). The assessment shall determine whether vulnerabilities that could lead to a single failure or to a common cause failure for engineered equipment are present. The assessment shall determine whether the structures, systems, components or barriers provided to carry out a safety function have adequate levels of redundancy, diversity, separation, segregation, equipment qualification, etc. as appropriate.**

Review Results

This Requirement is addressed. Redundancies are implemented. The single failure criterion is implemented [DCD F.0.3.1.2 and 2 P.2.1]. For systems responsible for heat transfer one system could be in repair or preventive maintenance could be performed. Common Cause Failures are taken into account in the Probabilistic Safety Assessment [DCD Ch. R.1.2.1.4]. In order to decrease the probability for Common Cause Failures the on-site emergency power results from two quite different diesel generator designs [DCD Ch. H.3-4]. Planned inspections and testing are reported. Thus an adequate level of reliability could be achieved. A rigid QA procedure is implemented.

As mentioned previously for 4.20, the identification of the SSCs is associated with the corresponding requirements that explicitly consider the different types of failure as well as their consequences for safety. Info on the single failure and common mode failures was not provided in the classification Chapter 3.2.

The EPR design is based on proven designs of operating reactors in France and Germany with some optimization. Thus much operating experience, experience with inspections and maintenance and many reliability data are available.

## 4.22–4.23 Site characteristics

**4.22 An assessment of the site characteristics related to the safety of the facility or activity shall be carried out and shall include:**

**(a) The physical and chemical characteristics that will affect the dispersion or migration of radioactive material released in normal operation or due to anticipated operational occurrences or accident conditions;**

**(b) The identification of the natural and human induced hazards of the region that have the potential to affect the safety of the facility or activity; and**

**(c) The distribution of the population around the site and its characteristics with regard to any siting policy of the State, the potential to affect neighbouring States and the need to develop an emergency plan.**

Review Results

The Requirement is addressed. Since no specific site has been selected, at this stage only generic site considerations and the methodologies for site-specific assessments could be addressed.

(a) The physical and chemical characteristics that will affect the dispersion or migration of radioactive material through direct and indirect pathways are a very site-specific issue. Results for the Flamanville-3 site are given as an example. Normal practices and future efforts to demonstrate compliance with HSE requirements will address this topic for a selected UK site.

(b) The document addresses the potential natural and human induced hazards typically considered in the NPP design. Since these hazards are site-specific, the discussion is centred around how these have been evaluated for Flamanviille-3 with indications on how it will be applied to a UK site. The EPR seismic design spectrum is defined as " EUR scaled to 0.25 g" and is designed to envelope nine ground conditions. If a future UK site condition is outside this range additional analyses will be needed. This follows the traditional practice in the siting of standard plants.

(c) The document concludes that for some existing sites, if similar demographic policy criteria were applied as to the UK Sizewell B site, the EPR would meet UK requirements. The RP states that the EPR's emergency planning meets the EUR, which is more stringent than the UK REPPIR requirements in broad terms. However, this does not constitute satisfaction of emergency planning requirements, and involvement on a specific basis from local authorities will be necessary.

It is recommended that the IAEA Safety Requirements No. NS-R-3 (2.22 through 2.25) or the equivalent HSE requirements be followed.

The discussion of hazards addresses the IAEA and international standards. Site-specific evaluations should be performed when a UK site is chosen.

**4.23 The scope and level of detail of the site assessment shall be consistent with the potential radiation risks associated with the facility or activity, the type of facility or activity to be carried out and the purpose of the assessment (e.g. to determine whether a new site is suitable for a facility or activity, to evaluate the safety of an existing site or to assess the long term suitability of a site for waste disposal). The site assessment shall be reviewed periodically during the lifetime of the facility or activity (see par. 5.10).**

Review Results

The Requirement is addressed. Since it is very specific to the site selected, at this stage only the procedures and methodologies for site assessment can be addressed. The procedures for selecting the site and identification and evaluation of hazards follow accepted industry practice and are in line with with the IAEA Requirements for Nuclear Power Plants (NS-R-3, NS-G-3.1, 1.5, 3.4, and 3.5).

The Requirement to periodically review the site assessment is not relevant at the time to new plant design.

# 4.24–4.26 Radiological protection provisions

## 4.24 The safety assessment shall determine whether adequate measures are in place for a facility or activity to protect people and the environment from the harmful effects of ionising radiation as required by the fundamental safety objective.

Review Results

The Requirement is addressed. Based on the assessments performed for the Flamanville-3 NPP the effectiveness of measures specified in EPR design is demonstrated by the fact that all calculated total doses to the most exposed groups are at least two orders of magnitude lower than the 1 mSv public dose limit. (Vol. 1 Ch. G)

Off-site doses in normal operation due to the management of the radioactive wastes and the provisions made to limit their release into the environment are described in Volume 2 - Chapter K. It is concluded that the liquid radioactive waste specific activity will remain low in comparison to the environmental samples' natural radioactive component. Radioactive waste will be treated and stored in a building on site and only final packaged radioactive waste, meeting the NII principals of containment, passive safety etc will leave the site by road or rail, complying with all relevant UK requirements for transport of radioactive materials by road or rail.

Radiological hazards under accident conditions are low as shown in discussion of Requirement 4.19.

The radiological consequences for possible incidents and accidents are as follows (Ch. E Section 3.2):

For PCC2 events it is postulated that the radiological consequences should not to be higher than those resulting from normal operation. In the UK, a legal limit of 1 mSv/yr is applied to the effective dose to any member of the public from normal operation of a nuclear facility. The effective doses due to EPR operation are expected to be only a small fraction of this level (see Vol. 1 Ch. G.2)

For PCC3 and PCC4 it is postulated that there should be no need for countermeasures for protection of the public (sheltering, evacuation, distribution of iodine tablets). To that end, the following limits have been agreed with the French regulator for Flamanville-3: effective dose < 10 mSv, thyroid equivalent dose < 100 mSv (Chapter 5.2.2.1).

The estimates for Flamanville-3 show that for DBAs the effective dose to children at 500 m from the reactor does not exceed 5.5 E-3 Sv, which is lower than acceptable doses in the UK.

The evaluation of the radiological consequences of severe accidents with core melt is described in Vol. 2 Ch. S.3. Considering a leak rate of the containment of 0.3% vol./day (maximum specified leak rate under design pressure and temperature), it is shown that the radiological objectives are met, i.e. evacuation or re-housing of population is not necessary; only sheltering in the immediate vicinity of the plant might be necessary, and the long term objectives are met by a large margin.

Preliminary results indicate Core Melt Frequencies for internal and external hazards of 8.4 E-8/reactor-year and 6.4 E-7/reactor-year respectively, showing compliance with the probabilistic objectives stated for hazards in subsection 5.1 of Vol. 2. Chapter R on Probabilistic Safety Assessment.

It is indicated that a comparison of the radiological consequences with the UK numerical targets and limits for accident conditions will be provided later in the pre-licensing process.

The implementation of the defence-in-depth concept is further discussed in Requirement 4.45.

**4.25 The safety assessment shall determine whether adequate measures are in place to control the radiation exposure of workers and members of the public within any relevant dose limit (as required by Principle 6 [1]) and that the protection is optimized such that the magnitude of individual doses, the number of people exposed and the likelihood of incurring exposures have all been kept as low as reasonably achievable, economic and social factors being taken into account (see Principle 5 [1]).**

Review Results

The Requirement is addressed. The ALARA approach is applied to minimize the radiological impact of plant operation on site workers and members of the public (Volume 1 Chapter E Section 3). The estimates are based on the assessments for the Flamanville-3 EPR.

Under normal operational conditions, radiation exposure of workers is minimized ALARA by the design provisions and measures described in Volume 2 Chapter L. These measures make use of experience accumulated in the operation of existing PWRs in France and Germany and concern, in particular, the following aspects:

a) Minimization of sources of radiation: As far as possible use of Cobalt-based hard-facing alloys, antimony and silver is avoided, primary coolant chemistry is optimized and purification systems (demineralizers, degasifiers) are designed to reduce the fission and corrosion products in the primary coolant to as low as practicable.

b) Layout: proper zoning, separation of high radiation components, provision of ease of access to components, shielding, setdown areas, ventilation paths, etc. (Vol. 2, Ch. L.3).

c) Maintenance and in-service inspection: Components design to reduce the frequency of maintenance work and the necessary effort involved per operation. potential reduction of doses during inspections and special provisions for most dose-inducing maintenance operations to reduce the time or number of personnel required to perform them and allow the use of removal aids (rails, rings, lifting gear) and remote control equipment (Vol. 1, Ch. F p.44-55)

To control exposure of the public in normal plant operation**,** the EPR project incorporates design improvements aiming to reduce the production of liquid chemical and radioactive effluent at source, as described in Section 3.1.1.1**.** They consist in the choice of materials limiting generation of radioactive elements (e.g. avoidance of cobalt). minimisation of sources that could give rise to isotopes such as Ag-100m, Sb-124, Sb-122 in the coolant, reinforced leak-tightness requirements, the use of boron enriched with B-10 but coupled to burnable poison assemblies for reactivity control of the reactor core, coolant pH control, enhanced filtration and ion exchange systems in the coolant clean up system. The mitigation measures aimed at abatement of radiological discharges from the EPR are described in Part D7.1.

The liquid chemical and radioactive effluent sorting and treatment circuits are designed to minimize the activities of liquid effluents that need to be discharged from the EPR and their subsequent impacts as described in (3.D.3.1.1.2). This includes an optimal recycling of borated primary circuit coolant, after it has been let down from the primary circuit (to allow boron dilution for reactivity control) and an optimal selective collection system for the different liquid effluents, controlling the production of tritium (3.1.2.1), reducing the liquid discharge of other radionuclides (fission or activation products) (3.1.2.2), reduction of process drains (polluted primary coolant, bleeds, equipment leaks) (3.1.2.3), improvement of the selective collection of floor and chemical drains (3 categories of floor drains) (3.1.2.4), and specific measures for chemical liquid effluent discharges associated with radioactive effluents

(3.1.3) such as reducing boron waste, lithium hydroxide, hydrazine and tritium (3.1.2.1) discharges.

To limit the impact of gaseous discharges the EPR design features are aimed at making use of best practical means at acceptable costs to minimize gaseous waste at the source and similarly in the abatement plant, and at balancing worker doses incurred in treatment in the plant with public doses from discharges (3.D.3.2, 3.E.9.2). The EPR's gaseous waste treatment system has a design that is similar to that of Konvoï reactors, and has the advantage of being able to treat aerated waste and to operate in an almost closed loop in normal operation. (3.D.3.2).

It is claimed that the EPR design and operational features will reduce liquid and gaseous releases in comparison to existing PWR 1300 MWe units as shown in Table E.9-a, b, c.

Doses to the public under accident conditions were discussed in Requirement 4.24. In case of severe accidents the frequency of core melt has been shown to be smaller than the INSAG targets referred to in the IAEA Safety Standards. In addition, following the ALARA concept, the EPR design includes features aimed at lowering the frequency of the most hazardous accident, namely a severe accident with containment bypass or early failure**.**

The design measures have resulted in decreasing the radiological consequences of steam generator tube rupture events. The delivery head of the Medium Head Safety Injection System (MHSI) is below the secondary safety valves set point, thereby reducing the amount of water which can be transferred from the primary system to the affected steam generator secondary side. The detection of the affected steam generator is based on a straightforward symptom (water level measurement). This initiates an automatic increase of the setpoint of the Main Steam Relief Valves which eliminates the primary-to-secondary leak. The steam generator secondary volume has been increased to provide a longer grace period with respect to the risk of water filling of the steam generator secondary side. As a result of design provisions it is claimed that there is no direct leakage into the environment (F.2.1.1.3).

Moreover, the major contributors to the PDS 3, i.e. the scenarios ‘practically eliminated’ due to design measures, include the initiating events of external heterogeneous dilution of the primary circuit due to the formation of a plug of unborated water, containment bypass situations (not including SGTR) for which it is assumed that core damage leads to a direct path between the primary system and the environment, and core damage situations involving damage under pressure. (Vol. 2 Ch. R 2.3.3).

Issues related to SGTR are further discussed in 4.45

**4.26 The safety assessment of the radiological protection provisions shall address normal operation of the facility or activity, anticipated operational occurrences and accident conditions.**

Review Results

The Requirement is addressed. Radiological protection provisions in normal operation are described in the assessment of Requirements 4.19 and 4.25, which has shown the EPR approach to address all respective IAEA Requirements.

Design basis events are analysed using a conservative approach to demonstrate that the radiological consequences of the postulated faults will remain low (5.2.2). This conservative approach is defined by a set of analysis rules and acceptance criteria which are detailed in Volume 2 Chapter P.1.0. In practice, rather than determining the effective dose in each sequence analysed, decoupling criteria are used, which apply to thermal-hydraulic parameters representative of the plant states reached during the fault sequences (5.2.2.1).

Provisions for severe accidents address measures for keeping the integrity of the containment. The main challenges to the containment integrity to be considered are hydrogen combustion, containment over pressurization, and corium-basemat (foundation raft) interaction,

Core melt scenarios are selected to be representative of the different in-vessel and in-containment physical phenomena. They are also chosen to provide boundary conditions for verifying the adequacy of the specific design provisions for mitigation of severe accidents.

Selection and the analysis of these scenarios are presented in Volume 2 Chapter S.2.2. The results are aimed at demonstrating that the envisaged design provisions are effective in preventing containment failure in cases of low pressure core melt, and that a sufficient time delay is available before operator action is needed.

The frequency of core melt with PDS 3 is estimated to be 9 E-8 /reactor -year (Vol. 2 Ch. R 2.3.3).

Besides sequences dealing with the reactor itself under all operational states, also the hazards due to spent fuel pool events are considered, including sequences leading to severe accidents. Vol. 2 Ch. R 3.2 presents the results of probabilistic analysis of accidents in spent fuel pool

## 4.27–4.37 Engineering aspects

**4.27 The safety assessment shall determine whether a facility or activity uses, to the extent reasonable, structures, systems and components of robust and proven design. Relevant operational experience, including results of root cause analysis of anticipated operational occurrences and accidents where appropriate, shall be taken into account.**

Review Results

The Requirement is addressed. The FSO documentation states that the EPR design has used several thousand reactor-years of operating experience, and the whole spectrum of knowledge acquired over the past forty years. It is claimed that the benefits of this feedback make it possible to have a very high level of availability (2.C.1.1.1). Relevant operational experience, including results of root cause analysis of anticipated operational occurrences and accidents, has been utilized in the development of the European Utility Requirements (EUR), which have been benchmarked against EPRI-URD, US regulatory requirements, IAEA Requirements & Guides and WENRA reference levels. The results of these benchmarks show that the EUR specifications offer a unified and high level of safety. The EPR design addresses the requirements of EUR.

New fuel assemblies have been developed for EPR, using previous operational experience and it is claimed that dimensional stability has been achieved (1.A.1.3).

Primary component support design is based on the design principles of the N4 unit. Important changes result from the implementation of the principle of Break Preclusion (2.E.4.9), depressurization of RCS and molten corium retention. The Break preclusion concept has been in use in modern NPPs for a long time and the systems and equipment used for this purpose are of proven design. The development work connected with the novel features of EPR is discussed in Requirement 4.29.

It is stated that the measurements taken on the HTP fuel assemblies as a whole have highlighted the absence of significant deformation. This satisfactory behaviour is attributable to the geometrical characteristics of the grid, which allow for satisfactory embedding of the fuel rods. The M5 alloy used for guide thimbles and the grids provides for significant margins even at very high burn up fractions, due to dimensional stability. (1.A.1.3)

**4.28 The safety assessment shall identify the design principles that have been applied to the facility and shall determine whether these principles have been met. The design principles applied would depend on the type of facility but could include requirements to incorporate application of defence-in-depth, multiple barriers to the release of radioactive material, safety margins, and the provision of redundancy, diversity and equipment qualification in the design of safety systems.**

Review Results

The Requirement is addressed. In comparison to the current generation of PWRs, the EPR design philosophy is based on the objectives to increase redundancy and separation, reduce core damage frequency (CDF), reduce large release frequency (LRF), mitigate severe accidents, protect critical systems from external events, improve man-machine interface (MMI), and extend response times for operator actions. These objectives are addressed through improved defence-in-depth, enhanced multiple barriers to the release of radioactive material, the provision of redundancy, separation, independence of redundant systems, diversity, introduction of passive features, larger safety margins, equipment qualification and new safety concepts.

Enhanced defence-in-depth includes larger safety margins for fuel and Reactor Pressure Vessel (RPV), break preclusion for RCS, improved overpressure protection at primary and secondary side, stronger containment protected against hydrogen hazards with Combustible Gas Control System which is completely passive, and core catcher to assure containment integrity after core melt. Inside containment, below the RPV, is a dedicated spreading area for molten core material following a postulated worst case severe accident. The cooling of the melt spread in the core catcher by the overflow of water from the IRWST is fully passive. Further discussion of defence-in-depth is provided in IAEA draft safety Requirement 4.45.

The principle of the melt arrest system is to achieve an automatic and fully passive transformation of the molten corium into a coolable configuration on the basis of simple physics and without requiring operator action or active internal or external systems. (2.S.2.2.4)

Redundancy and Separation: Redundant 100% capacity safety systems (one per Safeguard Building) arranged in four trains are strictly separated into four divisions.

Single Failure Criterion: The single failure criterion is fulfilled. For the components providing F1 functions, the single failure criterion is satisfied in order to ensure a sufficient level of redundancy. The power supply for components with an F1 function are backed up so that their functions can be performed in the event of loss of the external power supply.

Diversity: The two digital control systems are diverse and independent (1.F.3.6.2). The advantages and drawbacks of making use of two digital systems should be evaluated at the next step.

Safety Margins: The RPV, PZR, and SGs have relatively large volume-to-core power ratios, which results in increased safety margins (extended period for operator action e.g. in mitigation of SB LOCA, SGTR, loss of feed water including EFWS, 1.A.3,1). The internal volume of the Containment Building is larger relative to most existing PWR design, which reduces the peak pressure and provides 12 hours to actuate active heat removal systems. An

annulus of large volume between the inner and outer containment wall is kept at sub atmospheric pressure and provides an effective damping volume to prevent leakages outside the containment in case of leaks through the inner wall.

Increased safety margins are provided in fuel which shows lower heat flux and better cooling than the fuel in N4 NPP, which accommodates low leakage in/out management modes. (1.A.2.5.1). The design of the voluminous core contributes to reducing radial leaks, while the heavy reflector improves neutron economy (v.3, 1.A.2.5.1). There is also increased safety margin in primary side overpressure protection (1.A.1) and Secondary Side Overpressure Protection.

Actuation of safety systems, including safety valves, does not occur prior to reactor trip making use of the depressurizing effect of the reactor trip. This approach minimizes the number of valve actuations and the potential for valves sticking in the open position. (1:A.3.2)

New safety concepts are aimed at eliminating some hazards that could lead to severe accidents including SGTR mitigation (1:A.3.2), Break Preclusion. (1.A.3.2), and prevention of large early releases of radioactivity (1.E.5.2.3.) by ‘practical elimination’ of:

- high pressure core melt sequences resulting in unacceptable direct containment heating,
- fast reactivity accidents,
- in and ex-vessel steam explosion phenomena,
- hydrogen detonation,
- severe accident sequences involving containment bypass,
- fuel melt in the spent fuel pool.

**4.29 Where innovative improvements beyond current practices have been incorporated in the design, the safety assessment shall determine whether compliance with the safety requirements has been demonstrated by an appropriate programme of research, analysis and testing complemented by a subsequent programme of monitoring during operation.**

Reviews Results

The Requirement is addressed. For all innovative improvements beyond current practices incorporated in the design of EPR programmes of research, analysis and testing have been implemented and are reported to have shown positive results. No EPR NPPs have been so far in operation, but extensive monitoring programmes are established.

The fuel test programme has been successfully carried out showing that wear at the grid level is negligible (1.A.1.3)

The EPR RCS is based on N4 design, proven over many years of operation. The RCP design is based on N4 RCPs, with some improvements. The design of seals n° 1 and n° 2 is identical to that used with good operational experience on the N4 and CP1300 plants' RCP assemblies; the design of seal n° 3 is very close to that used on 900 MW plants' reactor coolant pumps. Some improvements have, however, been adopted for the EPR:

- pump operation at low pressure when the SIS/RHRS is connected to the RCS and is operating in residual heat removal mode
- absence of a back-up system for rapid injection at the shaft seals in the event of total loss of electrical power
- standstill seal system which can be activated when the pump is shutdown. 2.E.4.1

**The next step safety report should include clarification how these improvements have been tested and proven.**

The design of the EPR steam generator is based on that of the N4 steam generator.

In-containment Refuelling Water System Tank is protected against sump suction clogging. The description of measures shows that all measures proposed for PWRs have been addressed

Sump clogging prevention measures are described (1.A.4.2) including screen backwashing functions (1.A.4.2). Also use of suitable thermal insulation is planned. The proposed measures cannot be considered to be proven in practice; because the program of implementation of improved sump protection against clogging was started in French PWRs in 2004. Before that a series of experiments had been conducted in the period 1999-2003 in several test facilities. The measures proposed for EPR cover the whole spectrum of proposals made for sump protection. However, no rigorous demonstration of effectiveness of sump protection is provided in the documentation, the description is qualitative only. The issue should be clarified in more detail in the next step safety report.

There is a dedicated compartment to spread and cool molten core debris for long term stabilization (1.A.5.3). Processes and components involved in molten core cooling have been experimentally studied within several research programmes. The documentation claims that the results confirmed the approach to corium retention taken in EPR (2.S.2.2.4.2.3). Further comments to defence-in- depth are shown in Requirement 4.45.

The manufacturing of components for EPR in Olkiluoto 3 showed that unexpected difficulties can appear. One of them is due to the RCS piping dimensions being larger than in previous plants. This can involve manufacturing problems related to subsequent capability of testing and monitoring during operation. Those problems have been successfully resolved, but deserve attention. The requirements concerning ultrasonic testing are described in 2E.04 only in general terms, without details. In view of the difficulties in respect of detectability of defects in RCS piping a discussion of the existing experience and proposed measures should be provided in the next step safety report.

The steel used for the primary circuit piping at Olkiluoto 3 is a well-known austenitic (i.e. e. stainless) steel. During EPR construction at Olkiluoto it was found that the primary piping was not made to specification, namely the grain size of the steel was too big for the type of ultrasonic testing qualified by STUK to be applied at Olkiluoto 3. According to STUK, the manufacturer was not able to reach the criteria due to the big size of the forgings and the proposed forging and heat treatment size. When the shortcomings of the pipes became known, TVO and AREVA at first considered finding a new testing method which could be qualified by STUK [Nucleonics Week 42, 2006]. In December, however, AREVA announced that they had abandoned that approach and decided to refabricate some of the coolant lines. In March 2007 it became known that AREVA had decided to recast all eight pipelines (using the same type of steel) [TVO: Olkiluoto 3 – Current news in March 2007; www.tvo.fi]. Manufacturing of the new forgings is based on optimized heat treatment of the most critical areas of the forgings. STUK has accepted this because of changes in the manufacturing programme: In the new manufacturing programme, one hot leg is forged from one piece, whereas in the first programme, two hot legs were made of one forging and cut in two afterwards. Thus, the forging size is significantly smaller now which is expected to lead to better results regarding grain size – together with optimized forging and heat treating. This issue is not addressed in the documentation.

According to the requirements formulated in the documentation, “The layout and design of RCS equipment must allow in-service inspections and periodic tests to be carried out” (2.E.4.3.). Then the documentation states the requirements for forging rate and grain size “to satisfy a good ultrasonic permeability in order to assure in service inspectability” (2.E.3.8.2).

The next step safety assessment should include the consideration of the process of forging of main parts of the RCS, in the light of the experiences with EPR forgings in the recent past.

**4.30 The safety assessment shall determine whether a suitable safety classification scheme has been formulated and applied to the structures, systems and components. It shall determine whether it adequately reflects their importance to safety, the severity of the consequences of their failure, the need for them to be available following anticipated operational occurrences and accident conditions, and the need for them to be adequately qualified. The safety assessment shall also determine whether the scheme identifies the appropriate industry codes and standards and the regulatory requirements that need to be applied in the design, manufacturing, construction and inspection of the engineered features or for the development of procedures and in the management system of the facility or activity.**

Review Results

The Requirement is addressed. The classification of structures, systems and components, divided into mechanical, functional, and structural classification, are described [FSO Ch. C.2] and listed in extensive tables [FSO Ch. C.2] as well as event classification and acceptance criteria [FSO Ch. P.0.2.1]. All the software of the safety-classified programmable I&C should be outlined in more detail. The importance for safety is considered; probabilistic considerations and frequencies are used only to group events [FSO Ch. P.0] but not components.

It is claimed that all relevant regulatory requirements including seismic have been or will be used [Head Doc. Ch. H].

The project management and the quality assurance of the management are described [Head Doc. Ch. B].

The UK-EPR is mainly based on components and systems of proven design. Therefore, regulatory requirements and design codes have been applied before; they are under licensing review now in Finland and France. Nevertheless, a detailed list with regulatory requirements and industry codes and standards should be provided and assessed against related codes and standards in the UK at the next step.

**4.31 The safety assessment shall address the external hazards that could arise for a facility or activity, and shall determine whether an adequate level of protection is provided. This could include natural external events (such as extreme weather conditions, earthquakes and external flooding) and human induced events (such as aircraft crashes and hazards arising from transport and industrial activities) depending on the radiation risks associated with the facility or activity. Where applicable, the magnitude of the external events that the facility must be able to withstand (sometimes referred to as design basis external events) shall be established for each of the external hazards on the basis of historical data for a site. Where there is more than one facility or activity at the same location, the safety assessment shall take account of the effect of a single external event such as an earthquake or a flood on all of them and of the hazard potential presented by each facility or activity to the others.**

Review Results

The Requirement is addressed. Treatment of external hazards (section 6 of Chapter D) starts with a description of EUR requirements followed by how they are met for Flamanville and concludes with a discussion whether the requirements would likely be met for a UK site or further site-specific evaluation is needed. For example, it is concluded that the potential for liquefaction would be considered for any site defined as a 'soft' site. Similarly, external flooding and erosion could be a potential problem for some UK sites and would require further investigation. Another example is where it is concluded that the UK generic site envelope is likely encompassed by the EUR requirements (i.e. extreme rainfall).

Section 5.4.2.1 of Chapter F describes the additional seismic margins introduced in the design through load combinations (e.g., Design Earthquake plus LOCA from guillotine break of the Pressurizer surge line). Similarly, Section 5.4.2.2 describes the protection against aircraft crash through 'aircraft shell' design or proper separation between redundant systems.

Selection of the Design Basis Events will finally be based on site specific analysis taking into account the historical data for the site and will also comply with the UK requirements on minimum recurrence intervals for different hazards.

Frequencies of core damage caused by external hazards have been estimated for Flamanville using approximate methods, generic data and some specific analyses. The calculation of frequency of core damage caused by earthquakes at the site is not complete and hence is optimistic; it should have been integrated over the entire hazard curve.

At this stage of the preliminary design, the results of probabilistic safety assessment are only given as 'point estimates'. Detailed calculations are not shown; however, the estimated frequencies appear to be optimistically low. There is no discussion of uncertainties in the data and models. Understandably, the analysis is simplified; more detailed and UK specific analysis for each hazard is proposed by the Requesting Party.

All external hazards that could reasonably arise at a plant have been addressed.

The frequency of core damage should be calculated by proper integration over the entire hazard curve. When a UK site specific analysis is done, the uncertainties in the data and modelling should be fully treated**.**

**4.32 The safety assessment shall address the internal hazards that could arise for a facility and shall demonstrate whether the structures, systems and components are able to perform their safety function under the loads induced by normal operation, anticipated operational occurrences and accident conditions that have been taken into account explicitly in the design of the facility. This could include consideration of specific loads and load combinations, and environmental conditions (of temperature, pressure, humidity and radiation) imposed on structures and components by internal events such as pipe breaks, impingement forces, internal flooding and spraying, internal missiles, load drop, internal explosions and fire, depending on the radiation risks associated with the facility or activity.**

Review Results

The Requirement is addressed. The internal hazards considered include pipe leaks and breaks, failure of vessels, tanks, pumps and valves, internal missiles, dropped loads, internal explosions, fire and internal flooding. For different systems, protection against postulated internal hazards is provided as listed in Table 1 of 2.C.4.1. Deterministic evaluations for certain internal hazards are discussed in Chapter C.4. For certain hazards, probabilistic safety assessment is used to demonstrate low contribution to frequency of core damage. For the UK EPR, a plant specific risk evaluation of hazards is proposed. The internal fire risk analysis done for Flamanville is discussed in detail.

Design and evaluation for postulated internal hazards follow the accepted industry practice and combines deterministic and probabilistic approaches. They address the IAEA Requirements.

**4.33 The safety assessment shall determine whether the materials used are suitable for their purpose with regard to the standards specified in the design and for the operational conditions that arise during normal operation and following anticipated operational occurrences or accidents that have been taken into account explicitly in the design of the facility or activity.**

Review Results

The Requirement is addressed. The EPR design recognizes mechanical safety classes, each associated with defined standards (Vol. 1, Chapter F, sec. 3.1).

For the RCS, which is the highest class, a 'break preclusion' concept is applied (Vol. 1, Chapter E, sec. 2.3.3). This concept is based on a series of stringent requirements on design, materials and operation, and is well-established in a number of AREVA-reactors, both in Germany and elsewhere. The selected mechanical standard is the RCC-M, which is a well-established French standard (comparable to ASMEIII). In this standard, due attention is paid to the behaviour of material under transient and accident conditions. Materials have been selected according to Vol. II of the RCC-M (Vol.2, subchapter E, sec. 1.3).

Vol.2, subchapter E.4, describes the basis for the selection of the materials for main components, a.o. base materials and welding. Improvements over the past have been achieved by using only forged materials, no moulded anymore (Vol.2, subchapter E.2, sec. 3.1.1 ad d). The number of welds has been reduced. Attention has been paid to RPV weld material near the belt line, as it is most susceptible for radiation embrittlement.

The material has been chosen so as to minimize radiation doses for maintenance, e.g. reduced stellite in the RCS (Vol.1, Chapter C, sec. 5.1).

For the steam generator tubes, Inconel 690 TT has been proposed, which should alleviate the concerns of the earlier Inconel 600, which has caused many problems in SGs worldwide and led to an extensive SG replacement program. In comparison, Incoloy 800 - which has functioned as a very successful SG material for almost 40 years - has not been selected. The safety concern is that SG replacement causes unnecessary radiological burden on plant staff and contractors (ALARA-concern), hence, selection of the SG tube material should be further assessed in the next step safety assessment.

The material is planned to be followed through plant life, which enables early detection of ageing effects.

The conclusion is that the mechanical design and the material selection follow well-established international codes and standards, and have incorporated the experience gained over the past years.

The fuel material consists of low-enriched uranium-dioxide, with gadolinium as neutron poison, or MOX (uranium plus plutonium). The fuel material is addressed in subchapters D-3.2 and 2D-2. However, these sections do not contain sufficiently detailed information on the fuel material. Although most aspects that should be considered are mentioned, no assessment is possible on the basis of this section. Some important aspects such as fuel swelling, chemical effects, maximum fuel centre line temperature, and fission product release are not addressed (are imbedded in other issues, e.g. 'irradiation effects').

For the cladding, although the use of M5 cladding is mentioned, extensive design requirements are mentioned, but there is not sufficiently detailed information on the material to assess whether the requirements have been met.

Only very limited information has been provided regarding the control rod materials.

It is, however, anticipated that the fuel, cladding and control rods will be similar /identical to the fuel used in other AREVA designs. The conclusion is that the documentation is insufficient to assess the aspect of fuel and associated (i.e. cladding, control rods) materials. This should be part of the next step safety assessment.

Regarding the fuel material, in view of the longer fuel cycles planned and the associated high burn-up, attention should be paid to the amount of gadolinium used and its effect on the fuel base material in the detailed assessment. If load following is considered, special attention should be paid to the behaviour under the transients and, notably, to possible pellet-clad mechanical interaction (PCMI).

High burn-up has special considerations: RIA[1]-limits are not well-known, as are pellet clad mechanical interaction (PCMI)-limits. Validation of core analysis programs is often limited to a certain percentage of gadolinium (e.g. 6%), whereas applications may go beyond that (e.g. 10%).

[1] RIA = reactivity initiated accident (e.g., PWR rod ejection, boron dilution)

**4.34 The safety assessment shall determine whether preference has been given to a fail-safe design or, if this is not practicable, whether a means of detecting the failures that have occurred has been incorporated wherever appropriate.**

Reviews Results

The Requirement is addressed. The Reactor Protection System is based on fail safe design. The EPR reactor as a whole has the fail-safe feature because its power is reduced by negative reactivity coefficient in case of accidents.

Passive safety features have been introduced into some safety systems, in particular in the CGCS for hydrogen control and CHRS for corium cooling.

Means for detecting failures have been provided, including the RCS leakage detection system, which is the key element of break preclusion concept being one of the main features of EPR safety philosophy.

The requirements for in-service inspection are formulated in the documentation. The requirements for instrumentation and control systems also show that the failure detection issue has been extensively addressed in EPR design.

The difficulties in manufacturing the RCS piping mentioned in Requirement 4.29 are a testimony to the importance attached to reliable and timely detection of any deterioration of the RCS piping. It should be borne in mind, that the piping elements initially produced had no strength defects, only the grain structure was not satisfactory from the standpoint of effective in-service ultrasonic inspection. After remake the RCS elements have been found correctly improved.

**4.35 The safety assessment shall determine whether any time related aspects such as ageing, wear-out or life limiting factors, such as cumulative fatigue, embrittlement, corrosion, chemical decomposition and radiation induced damage, have been adequately addressed.**

Review Results

The Requirement is addressed. Vol. 1, Chapter F, sec. 3.1 (last paragraph) addresses time-related aspects of the design of SSC, such as number and duration of loading conditions, degradation caused by fatigue, corrosion and irradiation, and implementing a surveillance program to record transients and compare them with the design basis. Vol. 2, subchapter E-2, specifies also acceptance criteria for some phenomena. The acceptable usage factor is given as 1 for full plant life, which is relatively high (often, a limit of 0.5 is applied).

Degradation mechanisms including ageing are also considered in the design in other parts of the documentation (e.g. Vol. 2, subchapter C.4.2).

In addition, the RCC-M is followed, which determines inspection requirements during plant life effects of ageing, wear out, etc. Ageing will be followed for a number of components, where considered relevant (Vol.2, subchapter E.2, Table 3). It is also in the Technical Directives (e.g. in Vol. 2, Chapter C.1, Table 1). However, a dedicated and comprehensive Ageing Management Program, comprising all ageing effects for a series of structures, systems and components (SSC) with their supports, was not found.

The next step detailed assessment of the EPR, should study whether e.g. the grids used for in-service inspection are fine enough to timely detect component deterioration (e.g., the erosion induced wall thinning and following pipe rupture, as occurred in ANO-2 in 1989, which went undetected by the inspection program). The corresponding ASME XI requirements do not always cover such effects.

The next step detailed assessment should also study the corrosion and life-time effects of the fuel rod hold-down springs, which have caused problems in the past for some AREVA-reactors. Deterioration will result in fuel rod movement during start-up and some transients, and may result in fuel damage and, hence, releases.

An Ageing Management Program should be created for safety-relevant SSCs, which follows the ageing of these components in a pre-defined way during plant life.

The acceptable usage factor is given as 1; this should be compared to usual practices (often 0.5).

**4.36 The safety assessment shall determine whether the equipment essential to safety has been qualified to a sufficiently high level so that it will be able to perform its safety function in the conditions that it would experience in normal operation and following the anticipated operational occurrences and accidents that have been taken into account in the design.**

Reviews Results

The Requirement is addressed. The documentation includes clear requirements concerning equipment qualification for normal and accident conditions.

Primary side overpressure protection (OPP) is classified as safety-related and the equipment used for this function is qualified for liquid, steam, and two-phase flow operation (1:A.3.3).

Components providing an F1 function have to be qualified for the ambient conditions in which they must operate in order to perform this function. (2.F.8) The sequence of qualification of the seismic class 1 equipment (defined in Volume 2 – Chapter C.7) for accident conditions comprises a seismic test phase combined with irradiation and thermodynamic loadings (1.F.5.2.4.1).

Safety injection system and residual heat removal system have to be qualified for accident conditions under which they are designed to operate (2.F.3.0). The SIS/RHR system is designed and has to be qualified so that none of the accidents studied in Chapters P and S prevent the system from satisfactorily performing its safety functions. The forces caused by pressure waves, and the reaction forces resulting from rupture of an SIS/RHR injection line connection to the RCS, are taken into account (2.F.3.0).

The documentation states that I&C systems must be qualified depending on their safety role and to the ambient conditions in which they perform their mission (2.F.8). This qualification should be demonstrated in the next step.

There are still some remaining tests to be performed on the PRZ Relief Safety Valves. The Sempell safety valve has already been tested (flow rate, handling time) in accident conditions (discharge of steam, saturated and under-saturated water) using different full flow tests and analyses. Cycling tests (endurance) of the pilot have been carried out. The Sempell valve is also installed on a large number of German power stations but with a different pilot than that of the EPR PRVs. The correct operation of the main valve and its pilots will be confirmed during the Final Acceptance Tests at full pressure and temperature, with reduced flow and during the plant Hot Functional Start-up Tests (2.E.4.7). It is recommended that the results to be reviewed after the Final Acceptance Tests are completed.

**4.37 The provisions made for the decommissioning of a facility or the closure of a repository for the disposal of radioactive waste shall be specified and the safety assessment shall determine whether they are adequate.**

Review Results

The Requirement is addressed. Specific design features and processes that will facilitate the decommissioning and dismantling of the plant have been described including choice of materials; design provisions; limitation of radioactive contamination; prevention of chemical contamination; storage and retrieval of design, construction and operation information, documentation and records; and site layout to facilitate removal or dismantling of large plant items.

# 4.38–4.41 Human Factors

**4.38 The safety of facilities or activities will rely on actions carried out by operators. The safety assessment shall address all the human interactions with the facility or activity and shall determine whether the procedures and measures that are provided for all normal operational activities, in particular those necessary for implementation of the identified operational limits and conditions, and those required in response to anticipated operational occurrences and to accidents, ensure an adequate level of safety.**

Review Results

The Requirement is addressed. Human interactions with the facility or activity are discussed in Requirement 4.40. The human factors sections of the submission focus on the human-technical/engineering interfaces and the interface between human-procedures and guidance is not discussed in any detail. The Normal Operating Principles (2.M.2), Operating Principles in Incident and Accident Conditions (2.M.3) and Operating Principles for Severe Accident Conditions (2.M.4) define the major activities to be conducted; however, the design of the human factors of the supporting procedures is not detailed.

The 'Technical Directives (Guidelines) for the design and construction of the next generation of pressurized water nuclear power plants', however, state that "sufficient and appropriate information must be provided to operators for a clear understanding of the true state of the units, including severe accident conditions, and for a clear evaluation of the effects of their interventions" (2.C.1.A.2.3). The directives also state that within the human factors programme "operator guidance including suitable documentation and procedures, including computerized procedures, are developed consistently and integrated with other interfaces used by operators" (2.C.1.C.3e)

The submission also states that the design of documentation systems and the information used in operational management such as graphs (colours, readability of characters, spaces, image density, and page density) take into account the risk of human error (2.Q.2.2).

Although it will be the responsibility of the operating organization to develop procedures to cover all aspects of the operation of the plant it is normally expected that the designer will provide initial guidance. Future requests for information should include the requirement for information on procedure development. In addition it is recommended that the results of the PSA should be used in developing the operating procedures (DS 394 2.31, Draft Safety Guide on PSA).

**4.39 The safety assessment shall determine whether personnel competences, associated training and minimum staffing levels for maintaining safety are adequate.**

Review Results

The Requirement is addressed. The submission addresses personnel competences and staffing levels, however, the Requirement for support of training is not specifically addressed.

The Requirement for training is mentioned throughout the submission, however, the statements are very general in nature and contain no information on how the designer will support or provide guidance to the operating organization on training requirements.

No reference to the required competences for operating the plant could be found in the submission. The submission does include an outline of the tasks of supervisors and operators and others during operation, commissioning and outage (2.Q.3.1.2). The staffing level to operate the plant is addressed based on French experience (2.Q.3.1.2). Guidance or assumptions of the minimum staffing level to operate the plant during normal and abnormal operation is not specified.

Staffing levels (including minimum staffing requirements), competences and associated training will be the responsibility of the operating organization to specify to satisfy specific national regulatory requirements. It is normally expected that the designer would provide guidance and assumptions in these areas.

It is recommended that relevant information should be requested in any further submissions.

**4.40 The safety assessment shall determine whether the design and operation of the facility and the procedures for activities have addressed the requirements for human factors, including those related to the ergonomic design of all the areas, human–machine interfaces where operator actions are carried out, and future decommissioning and closure activities.**

Review Results

The Requirement is addressed (with the exception of procedures which are discussed in Requirement 4.38). The submission focuses on the process used to design and implement human-machine system interfaces and provides little information on the design of human-procedure/guidance interfaces. An exception is the provision of information in the form of alarm systems, plant information systems and data processing. The information presented to the operator and how it is organized is presented (2.Q.3.2.1 and 2.2); this also includes the alarm philosophy (2.Q.3.3).

The Human Factors Engineering (HFE) programme covers all aspects of the unit design and operation, and all stages of the plant life (including decommissioning) (2.Q.2). The scope of the HFE covers:

- Reactor Control activities - feasibility, measurability, failure recovery, human redundancy, appropriate training.

- Maintenance activities – layout of buildings and facilities provided, maintenance organization, maintenance procedures, limitation of maintenance, working environment.

The design process incorporates a HFE approach in the general plant layout and design (2.Q.2.5.3), this includes identifying areas or activities that are likely to be a problem based on experience feedback, and analysing future activities to check their feasibility and determine error probabilities. Analysis and corrective action covers:

- Operability and maintainability

- Security

- Transport and handling

- Hygiene and working conditions

- Communications, and

- Environmental protection

French and German operators of existing units have been involved in the preliminary detailed studies of Human Factors Engineering (2.Q.3.1). The view on Human factors of users and designers have been brought together and incorporated in the design. This applies to matters of structuring operational management by function, specifying operational management at primary-system level, the degree of automation, summary information, and operational principles during accidents (2.Q.3.2.2). Systems are designed with the objective to ensure that no operator action from the control room is required for the first 30 minutes after the initiating event. The principles and criteria for automating processes are well defined (2.Q.3.1.3).

Operating principles cover the centralized control of the process (Main Control Room), local control rooms, Remote Shutdown Station (RSS), and the Technical Support Centre (TSC). The Human Machine Interface Equipment within these centres, together with their functions are specified in the submission (2.Q.4.1).

Information on the provisions in the site layout to facilitate removal or dismantling of large plant items is specifically highlighted within the submission for decommissioning (1.F.8 and 2.T)

Information on the design and format of procedures and guidance is not provided. It is recommended that further information should be requested in any future submissions.

## 4.45–4.48 Defence-in-Depth and Margins

**4.45 The assessment of defence-in-depth shall determine whether adequate provisions have been made at each of the levels of defence in order to ensure that the system can:**

- **(a) Address deviations from normal operation and, in the case of a repository, from its desirable long term evolution;**
- **(b) Detect and intercept safety related deviations from normal operation and the desirable long term evolution should they occur;**
- **(c) Control accidents within the limits established for the design;**
- **(d) Identify measures to mitigate the consequences of accidents that exceed design limits; and**
- **(e) Mitigate the radiation risks of possible radioactive releases.**

**4.46 The safety assessment shall identify the necessary layers of protection including physical barriers to confine radioactive material at specific locations and the need for supporting administrative controls to achieve defence-in-depth. This shall include the identification of:**

- **(a) Safety functions that must be fulfilled;**
- **(b) Potential challenges to these safety functions;**
- **(c) Mechanisms giving rise to these challenges and the responses to them;**
- **(d) Provisions made to prevent these mechanisms from occurring; and**
- **(e) Provisions to mitigate the consequences if the safety function fails.**

**4.47 In order to determine whether defence-in-depth has been adequately implemented, the safety assessment shall determine whether:**

- **(a) The priority has been given to: reducing the number of challenges to the integrity of layers of protection and physical barriers; preventing the failure or bypass of a barrier when challenged; preventing the failure of one barrier leading to the failure of another one; and preventing significant releases of radioactive material if failure of the barriers does occur;**
- **(b) The layers of protection and physical barriers are independent of each other as far as practicable;**
- **(c) Special attention has been paid to internal and external hazards that have the potential to adversely affect more than one barrier at once or to cause simultaneous failures of safety systems; and**
- **(d) Specific measures have been implemented to ensure the reliability and effectiveness of the required levels of defence.**

**4.48 The safety assessment case submission should justify that shall determine whether there are adequate safety margins in the design and operation of the facility or activity in normal operation and under anticipated operational occurrences or accident conditions so that there is a wide margin to failure of any structures, systems or components for any of the anticipated operational occurrences or accident conditions that could occur. Safety margins are typically specified in codes and standards as well as by the regulatory body. The safety assessment shall determine whether acceptance criteria for each aspect of the safety analysis are such that an adequate margin is ensured.**

Review Results

The Requirements are addressed. Defence-in-depth is addressed in Head Document, Chapter C, Sec. 4. Reference is made to the Technical Guidelines, which are based on the common safety approach by RSK/GPR. The focus of these documents is, however, on severe accidents rather than the whole concept of DiD.

Volume 2, subchapter C.1, sec. 1.1.2, addresses the concept of DiD in more detail. As the EPR is a further development of the existing PWRs but is based on the same technology, the concept of DiD is inherently present. It is also explicitly visible in e.g. the classification of initiating events and their different acceptance criteria, as described in Vol. 2, Chapter P, subchapter P.2.

Some changes, however, have been introduced, as is described below:

Advances in technology have changed the design basis: LBLOCA is ruled out due to the 'break preclusion' concept, and SBLOCA is treated by secondary side measures. Consequently, the ECCS functions have been redefined, e.g. the High Pressure Safety Injection (HPSI) as been deleted from the ECCS design. For containment design, however, the LBLOCA has been retained.

To delete the HPSI has an important safety benefit: it reduces the probability of SG overfill in the case of an SG tube rupture and, hence, the probability of containment bypass. The negative consequence is that injection at nominal or near nominal pressure is impossible, i.e. the function of depressurisation is extremely important for successful injection by the ECCS in the case of a SBLOCA. However, the RP claims that "Due to the more favourable design of the reactor pressure vessel which reduces the extent of core uncovery in the case of the small LOCA, it has been possible to reduce the injection pressure of the HPSI (now referred to as the MHSI) below the SG safety valve set point, achieving a reduction in SG overfill risks compared to existing plants and avoiding the risk of liquid discharge through the safety valves".

As the safety benefit of the proposed changes did not become clear from the documents studied, a detailed assessment - which is outside the scope of this task - is needed to substantiate it.

Apparent good options in the EPR which strengthen the DiD-concept are listed in Vol. 1, Chapter C, Sec. 4.2.4. The list presents various passive safety improvements. A good example e.g. is the added volume to the SG and pressurizer, making the system less sensitive to secondary disturbances (e.g. no lifting of primary SRVs in response to secondary disturbances which otherwise could result in a stuck-open SRV (TMI-2 accident).

A good practice in PWR-design is the functioning of control systems so as to avoid actuation of safety systems. I.e., control systems (not classified for safety) can handle many events and prevent, thereby, actuation of safety systems that would otherwise come into action. I.e., the first level of defence in the DiD-concept is strong. Although AREVA-reactors in the past have been designed for this function, it is unclear from the documents studied whether this approach has been retained.

The DiD level 1 is further strengthened by the following elements:

- possibility to decouple from the grid and carry ‘island operation’ (Vol. 2, Chapter 2.H);
- a main and an auxiliary grid connection (Vol.2, Chapter 2.H); and
- emergency shutdown room as backup of the main control room (Vol.2, Chapter 2.G.2).

A typical feature of the handling of an SGTR in the EPR is that, during the primary depressurisation, the affected SG is not isolated. i.e., certain releases are permitted. Although this feature is common in AREVA-designed PWRs, it is not a necessary feature.

Some PWR designs have an early isolation of the affected SG and some AREVA-designed reactors adopted also this strategy. In this sense, the EPR resolution of the SGTR may not be in line with the ALARP principle. However, the acceptance of certain releases (which are still below acceptable limits) in the handling of the SGTR event reduces the risk for containment bypass, which, in the case of a degraded core condition, could lead to large releases. It is recommended that this feature should be analysed in more detail at the next step.

The DiD as formulated by the EPR is not fully consistent with the INSAG-formulation (to which it refers). Notably level 3 in INSAG addresses only accidents within the design basis, and accidents outside the design basis, including severe accidents, are addressed in level 4. EPR, in Vol. 1 (Head Document), Chapter 5.1 and Vol.2, subchapter C.1, sec. 1.1.2, treats all accidents in level 3, and places only severe accidents in level 4. This interpretation is not correct, because there are also accidents which fall outside the formal design basis, but for which still protection can and should be achieved. This is the class of Beyond Design Basis Accidents (BDBA). For a number of BDBAs, protection can be achieved by an appropriate use of operation and/or safety systems, together with proper instructions (mostly symptom-based Emergency Operating Procedures, SB-EOPs).

However, in the proposed classification of accidents, such accidents are fully taken into account. This is notably reflected in the introduction of Risk Reduction Categories (RRC), where RRC-A events span the BDBA discussed above. They are listed in Vol. 1, Table 5.6. The next step detailed assessment should reveal whether all relevant events have been addressed. An example of an event which often is considered is an SGTR followed by a SBLOCA. In principle, the selected basis of initiating events in Vol. 1, Table 5.6 should be acceptable, as it is derived from the PSA.

A good practice is also to classify the associated SSC as safety class F2, which is a class outside the formal safety classification for all events within the design basis but which still needs specific consideration in the design.

PSA has been used to help defining the range of relevant initiating events and credible additional complications. It has also been used to strengthen the DiD, as is explained in Vol. 1, Chapter C, sec. 4.3.

In the matter of severe accidents, extensive measures are taken to mitigate their potential consequences; for example, consideration has been given to H2-generation and a melt-spreading and cooling device has been designed. The EPR design apparently takes full credit for the associated analysis codes and other supportive arguments, as it has deleted the vented containment possibility (either filtered as in many operating AREVA-designs, or unfiltered as in US-designs) from the design. Such venting maybe needed if, despite the presence of debris cooling equipment, corium-concrete interaction will occur and, hence, non-condensable gases will be generated (CO, CO2, H2 – see further in this text).

The concept of the EPR corium cooling is based on two presumptions:

1. the molten corium mass has sufficiently low viscosity so that it will flow over the entire floor space of the expanded cavity;
2. the corium layer will be so thin (around 10 cm) that it can be successfully cooled from an overlying water pool.

Since the effectiveness of the EPR core catcher system in assuring the arrest of a molten core of around 250 tons of material has not been fully demonstrated in the documents presented for this review, the justification of the concept should be part of the next step safety assessment. This justification should include the following steps:

1. Consideration of the effect of accident management actions to put water on the core in earlier stages of the accident, as this is the action usually foreseen in severe accident management guidelines (there are not yet such EPR-specific guidelines). Note that no a-priori overview is possible of the total volume and effect of such actions, as they depend on the availability of pumps and water sources, attempts to restore lost equipment back to service (which can be partly successful, or successful for some limited time only), and operator actions (either correct or wrong actions), which makes it difficult to predict the actual characteristics of the corium that fails the vessel. Note that the claimed low viscosity of the corium mass is a necessary condition for the success of the EPR corium cooling concept, as otherwise spreading of the corium will be incomplete and cooling may not be fully achieved.

2. In addition, the corium inside the vessel may be stratified, as has been seen in the RASPLAV and MASCA experiments. Type and degree of stratification depends on the composition of the corium material, and is notably influenced by the presence of other elements such as carbon and iron. The stratification may influence the composition of the corium that leaves the vessel.

3. The coolability of the corium mass by an overlying pool of water should be justified, also in the light of the experimental work in this area (e.g. MACE-tests and later programs, as discussed in the OECD GAMA framework). Reference to the coolability of the TMI-core is not appropriate in this case, as the cooling mechanism there included cooling from below (existence of a gap between the vessel wall and the corium crust). There is also a scaling problem, as the molten mass for the EPR is substantially larger than that of TMI and thermal-hydraulic conditions (e.g. high pressure in TMI) are different.

Even if justification cannot be fully given, the concept still is considered to be useful as it will delay or reduce the amount of core-concrete interaction that otherwise (i.e. without such as device) will occur. In that case, however, the generation of non-condensables should be taken into account. Note that these gases may also influence the behaviour of the containment cooling device.

It should also be realized that a severe accident cannot be considered controlled unless all debris is covered and cooled, including the debris that is still inside the vessel. This requires flooding of the core catcher volume plus the annual space around the reactor to above top-of-active-fuel (TAF). This will result in a pressure rise in the containment.

Hence, two processes can be defined that increase the pressure in the containment by non-condensables:

- core-concrete interaction, if there is only partial success of the corium cooling concept;
- flooding the lower part of the containment in the long term mitigation.

The design, however, does not provide for a dedicated venting capability at elevated pressure. Note that normal ventilation ducts are not suitable for such venting as they usually can only withstand atmospheric pressure. The next step safety assessment should consider this matter in more detail.

Another feature for consideration in severe accidents is the containment spray system, as this is the only system capable of mitigating containment bypass scenarios. The containment spray is designed for control of pressure and temperature and removal of fission products from the containment atmosphere in a severe accident (it is not designed to function in DBA, hence, it is of reduced size compared to the 'usual' containment spray; Head Document, Chapter F, p. 13). The next step safety assessment should investigate the benefit of this system for containment bypass scenarios, in view of the limited size of the system.

Hydrogen combustion has been taken into account, and devices are in place to prevent the global H2 concentration to exceed 10%. Also inhomogeneous hydrogen concentrations have been considered (Vol. 2, sec. 2.5.2.2.3), including flame acceleration and transition to detonation from such flame acceleration (DDT - deflagration tot detonation transition). The effect of inhomogeneous distributions should be considered carefully in the next step safety assessment, as local hydrogen concentrations have been calculated up to 16%. Additional studies should be done to include the H2 generated in core-concrete interactions, unless the corium cooling concept can be fully justified.

Mixing is achieved by connecting the various containment compartments. As this is achieved by passive means only, i.e. by the pressure and temperature effects of the ongoing accident, it should be substantiated that the required openings indeed take place and no active measures need to be provided (as are provided in some existing AREVA-PWRs).

A rationale behind the EPR position may also lie in the Technical Guidelines, which require flame acceleration studies if the H2-concentration can be above 10% (Vol. 2, subchapter C.1, sec. E.2.2.4). Despite this rationale, the reviewers have the opinion that the safety case by the applicant should be fully self-contained and not rely on statements by respected bodies. This applies also to their statement about the unacceptability of igniters for hydrogen mitigation. A plus is that the Requesting Party is aware of the uncertainties involved.

The next step safety report should provide further clarification of the issues of inhomogeneous hydrogen concentrations, flame acceleration and possible DDT - deflagration to detonation transition, and also give justification for the absence of igniters for hydrogen mitigation. It should be noted that flame acceleration /DDT may only be relevant for remote scenarios. In that case, probabilistic arguments could be added to the severe accident management considerations. A common approach in this area is the ROAAM approach, developed by Prof. Theofanous.

A typical feature of the EPR is the so-called 'dry cavity' design. The common understanding

in severe accident mitigation is that a wet cavity is to be preferred, as it either can prevent vessel melt-through (for low-power reactors) or delay it (for high power reactors) and, when melt-through still may occur, mitigate the consequences. The residual risk of ex-vessel steam explosions is at present under study in the OECD-GAMA framework. EPR does not take any advantage of the 'wet cavity' concept and accepts a-priori a vessel melt-through.

The next step safety assessment should investigate whether this concept indeed brings substantial benefits over the 'wet cavity' design. Vol. 1, Chapter C. Sec. 4.2.3 even states that the core has to be cooled outside the vessel *on the basis of the DiD-concept*[2], without any further substantiation.

Reviewers anticipate that a core melt from full power without any successful mitigative action cannot be stopped inside the EPR RPV by external flooding, but for a core melt from partial power and/or after various partly successful interventions by the operating personnel external flooding may be a successful preventive strategy. In addition, as with many existing PWR-designs, such strategy may be considered useful by the TSC in executing severe accident management guidance (SAMG). The strategy, hence, should be subject of the next step safety assessment and, possibly, considered by the designers. In case of such change, the hazards of ex-vessel steam explosions should also be addressed in the next step safety assessment.

Severe accidents also require appropriate accident management procedures or guidelines, usually known under their acronym SAMG (Severe Accident Management Guidance). Such guidance deviates from Emergency Operating Procedures (EOPs), as it focuses fully on the protection of the (remaining) fission product barriers, eventually without taking notice of the protection of the plant itself. No evidence has been found that such instructions, specifically designed to mitigate severe accidents, have been developed or are under development. In Vol. 2, subchapter M.3, sec.3, severe accident management is mentioned, but there is no reference to the actual SAMG.

As an example, a relevant issue for SAMG will be the starting time / duration of a passive containment cooler, as it contributes to de-inertisation of the containment atmosphere. The applicant has recognized the issue in his reference to the Technical Guidelines (Vol. 2, Chapter C.1, sec. E.2.2.4), but not developed the appropriate operator guidelines to consider this issue in a real event. Another example is the possible priority to add water to the SG over the need to add water to the core, as in the Westinghouse Owners Group SAMG

In addition, SAMG measures are usually executed from what is mostly called the Technical Support Centre, which is a support centre specifically designed for this purpose. This centre has adequate instrumentation and documentation to enable responsible staff to carry out their duties in SAMG-domain. The next step safety report should address whether the EPR Technical Support Centre (Vol. 2, Chapter 2.G.2) is adequate for this function.

EOPs have been considered (Vol. 1, Chapter F, sec. 5.2.2.4; Vol. 2, subchapter M.3), but it is not fully clear how their actions are incorporated in the PSA and how they contribute to the DiD. Operators may omit actions that they should take and may make errors in things they do. For example, both actions of *omission* as well as actions of *commission* should be considered in the PSA. Whether this has been done must be part of a detailed assessment. There is no

[2] *Italics* by the authors

direct reference to operator actions, neither EOPs nor SAMG, in the description of DiD. EOPs usually belong to level 3 (DBA) and, in part, to level 4 (BDBA). SAMG are in the 4$^{th}$ level. An indirect reference to the DiD is present as EOPs should cover PCC 2 - 4 conditions and RCC-A.

A comparison to DS348, sec. 4.45 - 4.48, results in the following:

- sec. 4.45, items (a) - (e) have been addressed in the design; a number of questions can only be answered in a detailed assessment as indicated above.
- sec. 4.46, items (a) and (b) have been addressed; there is no explicit reference to items ( c) and (d), but such items appear in the PSA; as there is feedback from the PSA into the design, the items should be covered; item (e) is addressed.
- sec. 4.47, items (a) - (d) have been found in the EPR design, but it was not possible within the limited time available to see whether the issues are covered to full depth.
- sec. 4.48: safety margins are addressed in the EPR design, but in some areas detailed assessment is needed to substantiate them, and in some areas the margins may not be sufficient, as indicated above.

It is recommended that the issues of the omission of the HPSI, the treatment of SGTR and the margins in the severe accidents should be addressed in more detail in the next step safety assessment

In addition, the concept of DiD as formulated by AREVA, notably the transition from level 3 to level 4, is not in full conformance with the definition by the IAEA. The design, however, is in compliance with this definition of DiD.

The DiD-concept in the EPR should be carefully analysed, notably where important deviations occur from established practices, as discussed above. Notably the margins believed to be present in the severe accident domain need a careful analysis, as some margins may not have a solid basis in the present-day understanding of severe accidents.

In some cases, the safety case is based on advance-statements by the RSK/GPR committee (e.g. the omission of igniters as a possible solution to the H2-problem). EPR should present a fully complete safety case, and not derive its solutions from such advance-statements.

Efforts should be undertaken to design and implement procedures to mitigate the consequences of severe accidents, ‘SAMG’.

# 4.49–4.52 Scope of Safety Analysis

**4.49 The safety analysis shall assess the performance of a facility or activity in all operational states and, as necessary, in the post-operational phase and shall determine whether there is compliance with the safety requirements and regulatory requirements**.

Review Results

The Requirement is addressed. Information on the safety analyses performed is provided in Chapter P ‘Reference Operating Condition Studies’. The various operational states of the reactor are systematically grouped into 6 categories. The analyses include events associated with the fuel storage pool fuel handling and multiple failures in the nuclear auxiliaries building in an earthquake.

Regarding the post-operational state, Volume 2, Chapter T, ‘Decommissioning and Dismantling’ provides summary information on provisions included into the design to ensure the containment of radioactive materials and the minimization of radiation risk to workers and the public. The summary describes measures aimed at minimizing radioactive waste and radiation exposure during dismantling including choice of materials, design provisions, documentation and site layout.

Information is provided on how regulatory requirements are met. Each Chapter of the Design and Safety Report is preceded by the related Technical guidelines (TGs), i.e. the requirements of the French regulator, which are addressed. Chapter H provides information on the licensing reviews by the French and the Finnish Regulator and a comparison to the WENRA reference levels. An assessment of the design against UK ALARP principles will be included in the Pre-Construction Safety Report.

**4.50 The safety analysis shall address both the consequences arising from all normal operational conditions (including start-up and shutdown where appropriate) and the frequencies and consequences associated with all anticipated operational occurrences and accident conditions. The degree of detail of the analysis shall depend on the magnitude of the radiation risks associated with the facility or activity, the frequency of the events included in the analysis, the complexity of the facility or activity and the uncertainties inherent in the processes that are included in the analysis.**

Review Results

The Requirement is addressed. The methodology for estimating occupational exposure is described in Volume 2 subchapter L.4.3. A target of 0.35 man-Sv per reactor-year is assumed to be realistic. The methodology for estimating public exposure is provided in Volume 3 subchapter D.7 based on the conditions of the Flamanville site in France. Realistic estimates for effective doses to the public in the vicinity of the plant are given as 1μSv due to liquid waste and 3 μSv due to gaseous waste (slightly larger values for specific groups).

Detailed results of the accident analyses are presented in Volume 2, Chapter P. In addition to the design basis accidents the accident analysis includes, consistent with NS-R-1, specified accidents beyond the design basis, including severe accidents. Best estimate analysis is performed in this category.

Results of a Level 1+ PSA are briefly summarized in Chapter R and include low-power and shut-down modes and consideration of external hazards. Depending on the complexity and uncertainty in processes bounding assumptions are used. Since the design of the EPR is not yet finalized it is stated that the “Level 2 PSA model remains evolutionary.” The radiological consequences of severe accident scenarios are presented in Volume 2, subchapter S.2.3 to demonstrate compliance with the EPR design criteria.

In some areas only preliminary information is available. It is indicated that at the next stage more detailed information will be provided regarding an assessment of the design against the UK HSE SAPs. This will require additional accident analyses and the completion of a full-scope PSA.

**4.51 The safety analysis shall identify the anticipated operational occurrences and accident conditions that challenge safety. This needs to include all internal and external events and processes that may impact on physical barriers to confine the radioactive material or otherwise give rise to radiation risks [1]. The selection of events and processes to be considered in the safety analysis shall be based on a systematic, logical and structured approach and shall provide justification that the identification of all scenarios relevant for safety is sufficiently comprehensive[2]. The analysis shall be based on an appropriate grouping and bounding of the events and processes and shall consider partial failures of components or barriers as well as complete failures.**

Review Results

The Requirement is addressed. Vol. 2, Chapter P describes the selection and grouping of anticipated operational occurrences and accident conditions. Internal and external events are included. In line with the rules of a deterministic safety analysis partial or complete failure of components is assumed. It is stated in Vol. 2, subchapter C.2.3.2.5 that "due to the implementation of the break preclusion, it is considered that the probability of a guillotine break is actually very low. It is therefore analysed using the best-estimate rules" listed in the subchapter.

Severe accidents are analysed by using best-estimate methodology. In case of large uncertainties in phenomenological processes conservative bounding assumptions are made. The preliminary estimate of the impact of representative core melt sequences are presented in Vol. 2, subchapter S.2.2 including performance of design features aimed at retaining the molten core in the core catcher. Reference is made to related experiments and analyses as documented in the list of publications.

The systematic process of using PSA to analyse severe accidents is described in Vol. 2, Chapter R. It is stated that the initiating events are evaluated from "French or international feedback" and "failure probabilities of specific equipment". No further details are provided. Due to the break preclusion concept, 2A LOCA and 2A SLB accidents (between the SGs and the fixed points downstream of the MSIVs) are "considered sufficiently low not to require consideration in the PSA".

The safety analysis report should provide in-depth discussion of the issue of analysing 2A-LOCAs using best-estimate rules in the deterministic accident analysis and for excluding 2A-LOCAs and 2A SLBs from the spectrum of accidents considered in the PSA.

It is suggested to provide more information on the systematic approach for selecting initiating events for the PSA.

The detailed experimental results of provisions of retention of the molten core as documented in the extensive list of references will have to be reviewed in future steps.

---

[1] It should be noted that different terms are used for the internal and external events and processes for different types of facilities and activities. For example, for nuclear reactors, the term used is postulated initiating events (PIEs) whereas for radioactive waste safety, the usual term is features, events and processes (FEPs).

[2] In accordance with the IAEA Safety Glossary [5], the term scenario is used here to describe "a postulated or assumed set of conditions and/or events".

# 4.53–4.56 Approaches to Safety Analysis

**4.53 The safety analysis shall incorporate deterministic and probabilistic approaches, as required by the graded approach. These approaches have been shown to complement each other and both shall be used together to provide input into an integrated decision making process.**

Review Results

The Requirement is addressed. The EPR design uses both deterministic and probabilistic analysis, as it states in sec. 2 of the Head Document (HD), Chapter F: “the EPR design is developed primarily on a deterministic basis, complemented by the use of probabilistic assessment”. Examples are presented in the HD, Chapter C, sec. 4.2 and 4.3. In this way, it can be concluded that an integrated decision making has been applied in a number of design considerations. This should be further stipulated in the next step detailed assessment on the basis of more detailed documentation, including the PSA.

Notably in the area of design provisions for severe accidents, however, it did not become clear whether various design alternatives have been considered and integrated decision making has been achieved. This should be investigated in the next step detailed safety assessment.

It is suggested that the use of PSA is checked / expanded to the application of optimisation of system design. Possibly, this needs the establishment of SSC probability design targets, e.g. reliability target for certain functions. An example is the shutdown function, which often is designed to fail not more than once in 1E+5 years.

**4.54 The aim of the deterministic approach shall be to define and apply a set of conservative deterministic rules and requirements for the design and operation of facilities or the planning and conduct of activities. If these rules and requirements are met, they are expected to provide a high degree of confidence that the level of radiation risks to workers and members of the public arising from the facility or activity will be acceptably low. This conservative approach provides a way of compensating for uncertainties in the performance of equipment and humans with the aim of providing a large safety margin.**

Review Results

The Requirement is addressed. The Head Document, Chapter E sec. 3 and 5, and Chapter F describe a classification of events within the design basis accident area (DBA) in 4 Plant Condition Categories: PCC1 - PCC4, a risk categorisation for events beyond the design basis in 2 Risk Reduction Categories: RRC-A (BDBA but no core melt) and RRC-B (BDBA with core melt). The four categories PCC1-PCC4 are in safety class F1.

For the systems that cover RRC-events, a special safety class is introduced: safety class F2.
For each of the categories limits of radiation are specified (Chapter E, sec. 3), as well as design rules.

Reactor and core design and safety are conservatively calculated (Vol. 2 D 3), as well as thermal hydraulic characteristics (2D4) and reactivity parameters (2D5). The conservative methodology used to support the safety demonstration and in particular the plant condition categories (PCC) are described in detail in Vol. 2 P. Therefore, the analysis rules for the plant conditions categories (PCC) are part of the conservative methodology (initial conditions, identification of dominant parameters, uncertainties…) that supports the nuclear power plant's deterministic safety assessment. Basically, uncertainties can be considered in a deterministic manner or a statistical manner. The calculations of the radiological consequences are calculated with the same conservative assessment rules.

The classification is extensive: mechanical, functional, seismic and structural (Vol. 2, Chapter C).

The design rules follow generally applied methods. They have not been studied in detail in this review, but if followed throughout would provide appropriate safety margins. For RRC-A equipment, the applicant has taken up voluntarily to meet the design requirements of PCC 4, which will result in a robust design with appropriate safety margins.

As no stringent design rules exist for equipment designed to mitigate RRC-B-events, applicability of selected design rules should be studied on a case-by-case basis.

The choice of the residual heat curves recommended for the accident studies (BE for RRC-A, 1.645 $\sigma$ for PCC except for short term LOCA and 2 $\sigma$ for short term LOCA) should be justified with regards to the level of conservatism required for each accident category.
The combination of uncertainties in a statistical manner for its application with a conservative approach should be justified in detail.

Notably in the area of RRC-B events (severe accident), the selected design rules and margins obtained should be studied in detail, to confirm the safety margins which the applicant claims.

**4.55 The aim of a probabilistic safety analysis shall be to determine all significant contributors to the radiation risk from a facility or activity and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where they have been defined.**

In the area of reactor safety, the probabilistic safety analysis that is carried out uses a comprehensive, structured approach to identify failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. The probabilistic approach uses realistic assumptions whenever possible and provides a framework for addressing many of the uncertainties explicitly.

Probabilistic approaches may provide insights into system performance, reliability, interactions and weaknesses in the design, defence-in-depth and risk that it may not be possible to derive from a deterministic approach.

Review Results

The Requirement is addressed. (This Requirement is complemented by further Requirements of NS-R-1, in particular the Requirement 5.37).

PSA and associated probabilistic design safety targets are part of the general safety principles (Vol. 1, Chapter E, 5.4). Together with objectives on reliability of protection and safety systems, the global design safety targets (whole CDF<1E-05/reactor-year, CDF<1E-06/reactor-year for internal events, LERF<1.E-7/reactor-year) are more demanding than the INSAG targets referred to in the IAEA Safety Standards and those of the USNRC (referred to in the AP-1000 and ESBWR analyses). From the PSA results, risk reduction categories are elaborated for reducing the importance of relevant risk contributors. More detailed probabilistic safety objectives and design targets are given in the PSA report (Vol. 2 Chapter R).

A Level 1+ PSA has been performed, meaning a Level 1 PSA complemented with a Level 2 PSA of limited scope at the current stage. The commitment for further PSA work on Level 2 and 3 PSA to support the UK pre-licensing is made. The current PSA covers internal initiating events and internal and external hazards in all operation modes. The objectives address the IAEA Requirements and provide a consistent framework for a safe and balanced design. The particular objective of Level 2 aspect of the PSA has been to perform a quantification of the ‘early containment failures’, to help demonstrate, in conjunction with deterministic arguments, their ‘practical elimination’, in compliance with the Technical Guidelines (Chapter R.0.3). The PSA has been carried out during the design process in accordance with French regulatory requirements. Chapter C, 4.3 and 4.4 indicate the use of PSA in improving the design and in the demonstration of the ALARP principle. Overall results of the PSA are presented in Chapter F, ‘Overall Safety Demonstration’, Section 5.

The information on particular areas of the PSA, e.g. analysis of low power and shutdown operation, is not presented in any detail at this stage. In general, little information is provided on the key aspects of the applications of the PSA methodology. However, the documentation shows that the analysis objectives are overall accomplished. The finalized full scope PSA should be reviewed in detail at the next step.

The initiating event (IE) identification is based on French or international experience. A familiar list of IEs is provided. No other details on the process for identification and grouping are given. The list contains overall categories. The breakdown of the IEs, e.g. by LOCA sizes is provided with the PSA results. More importantly, guillotine breaks (2A) of primary and secondary circuits are excluded from the PSA due to sufficiently low frequencies based upon the break preclusion principle of the main pipework, which applies also the RPV, SGs and RCPs, that are considered unbreakable.

Accident sequence analysis is reported to be carried out with consideration of realistic plant parameters, data and thermal-hydraulic calculations. Accident sequences below 1.E-12/reactor-year are considered negligible.

Reliability data are derived mainly from operational experience from France and Germany, supplemented by the EG&G generic reliability database.

Methods employed seem to be consistent with common PSA Level 1 methodology, but few details are given. Exceptionally, the methods for calculating IE frequencies are explained. Separate consideration is made of the instrumentation and control system, for which a so called compact failure model is developed and the results are integrated as a generic event in the PSA even/fault tree models. The models of the I&C system seem to address failures of control functions which would lead to protective actions as well as actuations of instrumentation channels on system components before or in addition to protective actions.

A systematic analysis of initiating events and accident sequences with indication of contributions to CDF is provided. The result analysis is particularly used for some IE categories such as boron dilution and containment bypasses with insight on component failures and human errors. Importance are not used or shown for this purpose. The analysis includes results for low power or shutdown operation, but no specific information is provided on the analysis for these modes of operation.

There is no indication or evidence that sensitivity or uncertainty analyses have been performed.

A long-term probabilistic evaluation is undertaken to check for the absence of a cliff edge effect on transient periods of more than 24h; the damage sequences induced by initiating events whose recovery time could be greater than this limit are studied over the long-term.

There is little information about the methodologies applied for the analysis of hazards. Only quantitative global results are given for the relevant hazards. No insights can be gained on the adequacy of the methodologies and their application.

The process for developing the Level 1+ PSA is documented in some detail. The code MAAP is used with best estimate data as input to the model and realistic approaches. It is stated, that “given that the design of the EPR is not currently finalized, the Level 2 PSA model remains evolutionary, particularly in terms of realisation of the Level 1/Level 2 interface and definition of the supporting MAAP calculations”. Chapter R however, does not provide PSA results of accidental releases and consequences. Insights on the Level 2 and PSA results are provided in Chapter S on risk reduction categories. Overall results of the PSA are presented in Chapter F, ‘Overall safety demonstration’ Section 5.

## 4.57 Criteria for judging safety

**4.57 Criteria for judging safety that are sufficient to meet the fundamental safety objective and the fundamental safety principles established in Ref. [1] and the requirements of the designer, the operating organization and the regulatory body shall be defined for the safety analysis. In addition, detailed criteria may be developed to assist in assessing compliance with these higher level objectives, principles and requirements, including risk criteria that relate to the likelihood of anticipated operational occurrences or accidents occurring with significant radiation risks.**

Review Results

The Requirement is addressed. The IAEA Safety Standards do not specify criteria for the safety analysis, but require that these be established by the designer, the operating organization and the national regulatory body. General and detailed criteria for the safety analysis have been defined by the designer and the regulatory body addressing the applicable fundamental safety objective and fundamental safety principles established by IAEA SF-1. (At this stage no operator has yet been determined.)

Criteria defined by the designer**:** It is stated that the EPR has been designed to meet safety specifications developed by the French Nuclear Regulatory Agency (DGNSR) as set down in the EPR Technical Guidelines (TGs). The TGs are the results of a 20 year process of French and German co-operation with international participation. Detailed information is provided on how the TGs, adopted as requirements by the French Regulatory Body, are met. Each Chapter of the Design and Safety Report is preceded by the related Technical Guidelines (TGs), which are addressed.

The TGs are deterministic in nature. Deterministic Safety Analysis based on conservative assumptions has been performed to demonstrate compliance. It is stated that “due to the implementation of the break preclusion, it is considered that the probability of a guillotine break is actually very low. It is therefore analysed using the best-estimate rules” listed in Vol. 2, subchapter C.2.3.2.5.

PSA has been used as a tool to identify severe accident sequences and to optimize design features aimed at reducing their contribution to overall risk. At this stage a PSA Level 1+ is available only. Due to the break preclusion concept, 2A LOCA and 2A SLB accidents (between the SGs and the fixed points downstream of the MSIVs) are “considered sufficiently low not to require consideration in the PSA”. The probabilistic safety design targets used are CDF< 1.0E-5/reactor-year for all events, CDF<1.0E-6/reactor-year for internal events, and CDF with early loss of the radioactivity containment function< 1.0E-7/reactor-year. In practice more detailed intermediate objectives have been used as summarized in the Head Document Chapter F.5.6. Separate criteria related to the consequences of AOOs have not been established. Due to the present limitation of the scope of the PSA, estimates of individual risk are not available.

Chapter H provides information on the EPR licensing reviews by the French and the Finnish Regulator and a comparison to the WENRA reference levels.

Criteria defined by the national regulatory body: The UK HSE has established detailed “Safety Assessment Principles for Nuclear Facilities, 2006 Edition”. The SAPs contain

general and detailed principles including principles for assessment of fault analysis for design basis analysis, PSA and severe accident analysis. Numerical targets and legal limits have been established which include risk criteria that relate to the likelihood of normal operation, design basis fault sequences (including a separate category related to AOOs) and severe accidents.

Due to the difference in concepts the results of the accident analysis by the designer are not directly comparable to the criteria used by the UK regulator. Based on some limited analyses and extrapolation of results the designer is confident that the UK HSE numerical targets and legal limits will be met. It is stated in the Head Document that a demonstration of compliance with the UK ALARP principles will be addressed in the Pre-Construction Safety Report.

The design of the EPR is based on the TGs, which are mainly deterministic. At this stage a Level 1+ PSA only is available. Additional analyses will be needed at the next step to demonstrate that the expectations set out in the UK HSE SAPs are met.

It is suggested that the next step safety analysis report should provide an in-depth discussion of the issue of analysing 2A-LOCAs using best-estimate rules in the deterministic accident analysis and for excluding 2A-LOCAs and 2A SLBs from the spectrum of accidents considered in the PSA.

## 4.58–4.59 Uncertainty and sensitivity analysis

**4.58 The safety analysis incorporates, to varying degrees, predictions of the circumstances that will prevail in the operational or post-operational stages of a facility or activity. There will always be uncertainties[1] associated with such predictions that depend on the exact nature of the facility or activity and the complexity of the safety analysis. To the extent practicable the results of a safety analysis shall be robust, i.e. tolerant to uncertainties.**

**4.59 Uncertainties in the safety analysis shall be characterized with respect to their source, nature and degree, using quantitative methods, professional judgment or both. Uncertainties that may have implications for the outcome of the safety analysis and decisions made on that basis shall be addressed in uncertainty and sensitivity analyses. Uncertainty analysis mainly refers to the statistical combination and propagation of uncertainties in data, whereas sensitivity analysis refers to the sensitivity of results to major parameter, scenario or modelling assumptions.**

Review Results

The Requirement is addressed. Uncertainties for the thermal-hydraulic core design are described in detail [DCD2 D4Ch.2.8]; a statistical as well as a deterministic approach is used for the Critical Heat Flux [DCD 2 D4Ch. 2.8.1].

The overall system uncertainty covers uncertainties in physical parameters measured during operation, code uncertainties for steady-state and transient calculations, and uncertainties related to fuel [DCD 2 D4Ch.2.8.2, DCD 2 D.4 Tab.3].

The uncertainties evaluation and treatment called for supporting the safety analysis should be analysed in depth. This applies especially to their estimation, combination (statistic and deterministic), including an in-depth review of their potential systematic deviation, propagation during transients and consequences on the results of the safety analysis for DBA and BDBA sequences. This might call for sensitivity analyses and scaling effects studies, which have to be assessed carefully.

For the Risk-Reduction Categories RRC-A a probabilistic methodology is used [DCD S Ch.0.1.1] while in sequences with core melts RRC-B mostly a deterministic approach is applied [DCD 2.S.2.1.1].

Sensitivity studies with safety codes are not reported and should be provided for detailed review at the next step.

[1] There are two facets to uncertainty: aleatory (or stochastic) and epistemic uncertainty. Aleatory uncertainty has to do with events or phenomena that occur in a random manner such as random failures of equipment. These aspects of uncertainty are inherent in the logic structure of the probabilistic model. Epistemic uncertainty is associated with the state of knowledge relating to a given problem under consideration. In any analysis or analytical model of a physical phenomenon, simplifications and assumptions are made. Even for relatively simple problems, a model may leave out some aspects that are deemed unimportant to the solution. Additionally, the state of knowledge within the scientific and engineering disciplines may be incomplete. Simplifications and lack of knowledge lead to uncertainties in the prediction of outcomes for a specified problem.

## 4.60 Use of computer codes

**4.60 The computer codes used in the safety analysis shall undergo verification and validation to a sufficient degree. Verification refers to the process of determining whether the controlling physical equations and data have been correctly translated into the computer code. Validation refers to the process of determining whether the mathematical model is an adequate representation of the real system being modelled by comparing the predictions of the model with observations of the real system or experimental data. The validation process shall identify the uncertainties, the approximations in the models, and shortcomings in the models and the underlying data basis and how these are to be taken into account in the safety analysis. In addition, users of the code shall have sufficient experience in the application of the code to the facility or activity being addressed.**

Review Results

The Requirement is addressed. All main components of the UK – EPR are of proven design. Only the mitigation features in case of postulated core melt scenarios are of novel design.

The codes used for the thermal-hydraulic and neutron design are listed [DCD Ch.D1, Tab.2; DCD Ch.D4 4.3]. No comparisons are presented between SMART code calculations and operational or experimental data at high burn-ups. An Initial Test Program [DCD Vol. 2 D2, D3, D4, D5] will aim to validate several thermal-hydraulic and neutron data.

The MAAP code was used [DCD Ch.R 2.2] to obtain the success criteria for the Level 2 PSA.

The experiments and the codes developed and used for sequences with core melt and the behaviour of mitigating measures are described [DCD Ch.S 2.4]. For determining the containment response to Severe Accident Scenarios much R&D work has been performed. The mixing of fluid corium with water inside the vessel has been studied in several experimental facilities; related computer codes are MATTINA and MC3D.

Based on experiments it is claimed that due to low flow rates the molten corium water interactions does not lead to high-energy interactions capable of challenging the containment integrity.

The hydrogen production and the mass and energy release from the reactor coolant system are calculated with MAAP. For the gas (hydrogen and others) and temperature distribution within the containment the GASFLOW code (with about 100.000 cells) has been used; it is described that this computer code has been validated using many experiments. This code is also used to study the effects of recombiner units. If deflagration cannot be excluded calculations with the COM3D computer code (with more than 1.000.000 cells) were performed to study dynamic effects [DCD 2 S 2]. The instrumentation needed to address these scenarios is described [DCD Ch. S 2. 2.6].

Comparisons between experiments and code calculations should be presented. Scaling considerations should be outlined for detailed review at the next step.

## 4.61 Use of data from operating experience

**4.61 If warranted by the potential radiation risks associated with a facility or activity, data on operational safety performance shall be collected and assessed, including records of incidents such as human errors, performance of safety systems, radiation doses, generation of radioactive waste and effluents. The scope of the data collection shall be commensurate with the graded approach. For complex facilities, the collection of data shall be based on a set of safety performance indicators that have been established for the facility. Operational safety experience shall be used, as appropriate, to update the safety assessment and to review the management systems; this is further described in Section 5.**

[5.10 The safety assessment and management systems by means of which it is conducted shall be periodically reviewed at predefined intervals in accordance with regulatory requirements. In addition to such periodic reviews, they shall be reviewed and updated:

(a) When there is any significant change that particularly affects the safety of the facility or activity;

(b) When there are significant developments in knowledge and understanding (such as those arising from research or operational experience);

(c) When there is an emerging safety issue due to a regulatory concern or an incident; and

(d) When there have been significant improvements in the computer codes or the input data used in the safety analysis.]

Review Results

The Requirement is addressed. The submission describes how Operating Experience has been utilized in the design; this includes recent significant issues within the nuclear industry such as sump blockage, essential supplies, and hydrogen detonation. The submission does not discuss the need of the licensee to maintain data records for future safety assessments during the operating life of the plant.

Chapter H of the Head Document states that in designing the EPR it was decided to follow an evolutionary approach: the advantage of basing an advanced design on operational experience from approximately 100 nuclear power plants in the world (Belgium, Brazil, China, France, Germany, Korea, South Africa, Spain) constructed by Framatome and Siemens was deemed by the designers to be very important.

In addition, experience feedback from other nuclear power plants has been reviewed and design features addressing the generic safety issues identified have been taken into account. The following examples illustrate this approach:

- SG tube integrity
- Overfilling of SG
- ECCS sumps blockage
- SG feedwater system availability
- Improved reliability for the power supply system

- Design measures dealing with hydrogen detonation, direct containment heating, vessel lift, ex-vessel steam explosion, basemat (foundation raft) melt-through, containment pressurisation and containment leakage.

A systematic review has been carried out to confirm that the EPR design addresses generic issues identified in IAEA-TECDOC-1044, ‘Generic Safety Issues for nuclear power plants with light water reactors and measures taken for their resolution’. A similar review in regard of NRC generic safety issues (NUREG 09333) is in progress for a US EPR in the framework of USNRC Design Certification.

Chapter H also highlights that EDF and AREVA, who are co-applicants for Generic Design Acceptance for the UK PWR, remain actively aware of international developments in reactor design, operation and regulation through participation in a range of international organizations. In particular EDF is a member and active participant in the World Association of Nuclear Operators and AREVA chairs the Framatome Reactor Owners Group.

## 4.62–4.65 Documentation

**4.62 The results and findings of the safety assessment shall be documented, as appropriate, in the form of a safety report, reflecting the complexity of the facility or activity and the radiation risks associated with it. The purpose of the safety report is to present the assessment and the analyses that have been carried out to demonstrate that the facility or activity is in compliance with the fundamental safety principles and the requirements established here and any other safety requirements set out in national laws and regulations**.

Review Results

The Requirement is addressed. Detailed documentation was available for the review. It consisted of a 'Head Document' (Vol. 1) specifically aimed at addressing the requirements of the UK HSE Step 2 request. The Head Document is complemented by detailed safety analyses contained in the 'Design and Safety Report' (Vol. 2) and the 'Environmental Impact Report' (Vol. 3). Vol. 2 is based on the publicly available parts of the French Preliminary Safety Report for the Flamanville-3 EPR. Vol. 3 is based on the Environmental Assessment for the Flamanville-3 EPR. The Head Document provides precise guidance on where more detailed information and results of relevant analyses are provided in Volumes 2 and 3.

The documentation is structured in accordance with the EPR Technical Guidelines (TGs). Information is provided on how the TGs, adopted as requirements by the French Nuclear Regulatory Agency (DGNSR), are met. Each chapter of the Design and Safety Report is preceded by the related TGs.

Safety approaches are presented in Ch. 1.E–Safety Principles and Criteria. Broad safety demonstration is presented in Vol. 1 Ch. F. which gives a synthetic view of the EPR safety case and more details are provided in Vol. 2. The operating principles in incident & accident conditions are presented in Chapter M.3, and for severe accident conditions in Chapter M4. Chapter P presents 'reference operating condition studies', including assumptions and requirements for analyses, plant characteristics used in the accident analysis, accident analyses and radiological consequences. Chapter R presents probabilistic safety assessment including safety requirements, level 1 and 2 probabilistic safety assessment, specific PSA and PSA regarding hazards. Finally risk reduction categories are presented in Chapter S.

Safety analyses are presented in Chapter 2.P, with assumptions and requirements for the plant conditions category (PCC) 2, 3 and 4 analyses, plant characteristics used in the accident analysis and radiological consequences. Event sequences involving multiple failures conditions that must be considered in the design, are grouped into Reduction Risk Category A (RRC–A) and considered on a deterministic basis (Vol. 1 Chapter F Table 5-6). A second stage in risk reduction involves analysis of a set of low pressure core melt scenarios (RRC-B severe accidents) that are not 'practically eliminated' in the plant design, and are presented in 2.S.2 and 2.S.3. The sequences are considered on a deterministic basis (Vol. 1 Chapter F Table 5-6). These scenarios are used to design the means of stabilizing and cooling the molten core when outside the reactor pressure vessel and for designing containment cooling systems which are claimed not to require a containment venting capability. They are also taken into account in the design of instrumentation used by the operator and the emergency response team to manage this type of situation, and to specify conditions for qualifying equipment needed to demonstrate achievement of safety objectives.

The Requirement 4.57 requests the establishment of criteria for judging safety by the designer, the operating organization (once it has been established) and the regulatory body. Due to the differences in concepts it is recognized by the designer that the results of the accident analysis are not directly comparable to the criteria used by the UK regulator. Based on some limited analyses and extrapolation of results, the Requesting Party is confident that the UK HSE numerical targets and legal limits will be met. It is stated in the Head Document that a demonstration of compliance with the UK ALARP principles will be addressed in the Pre-Construction Safety Report.

The probabilistic safety analysis prepared by the Requesting Party has been assessed in more detail in Requirement 4.55. The design of the EPR is based on the TGs, which are mainly deterministic. At this stage a Level 1+ PSA only is available. Additional analyses will be needed at the next step to demonstrate that the expectations set out in the UK HSE SAPs are met.

The review showed that in several areas more information will be needed to assess whether Requirements of the IAEA Safety Standards or the UK HSE SAPs have been addressed. These include e.g. categorisation of events/accidents, classification of safety functions/systems, and issues related to the PSA, which was only briefly summarized. These areas will need to be reviewed in more detail at the next step.

Also areas have been identified where additional information would need to be provided to support the claims made. In particular these include more details related to the use of the break preclusion concept, the removal of the HPSI, the technical basis for the performance of the core retention system below the RPV, the absence of a containment venting system, PSA related issues including the removal of LB LOCAs from the list of IEs, increased burn-up, extended plant life, uncertainty analyses related to core layout, stability analysis and scale-up considerations, and validation of computer codes. These areas would need to be reviewed in more detail at the next step.

**4.63 The quantitative and qualitative outcomes of the safety assessment form the basis of the safety report. These are supplemented by supporting evidence for and reasoning about the robustness and reliability of the safety assessment and its assumptions, including information on the performance of individual system components as appropriate.**

Review Results

The Requirement is addressed. Both quantitative and qualitative outcomes of the safety assessment are presented. The accident analyses in Chapter 2.P are concluded with a clear statement of the effects of the accident on plant systems and on radiological hazards. In Chapter 2.F.2 the robustness of containment and safeguard systems is described with the objective to demonstrate that the containment can withstand all accidents called in EPR project Risk Reduction Category A (RRC-A) accidents and RRC-B or severe accidents. The reliability of systems used for containment protection is claimed to be very high due to application of passive safety principles.

The robustness of safety analysis is shown by including in the containment load combinations in the case of 2A LOCA, which is the guillotine break of a primary cooling system cold leg (1.3.2.2). This accident has been removed from the design basis, but has been maintained for the containment design. The maximum pressures and temperatures are 4.3 bar and 182°C, occurring at 20 s. (2.F.2.1.3).

In contrast to previous generation nuclear power plants, the EPR containment design addresses the possibility of core meltdown accidents involving low-pressure vessel rupture, and aims to prevent leakage from the reactor building into the environment in such accidents (2.F.2.1.0.1). For core meltdown accident sequences which may occur during shutdown states with an open containment, the containment must be capable of being closed with an acceptable reliability before the occurrence of a large radioactive release (2.F.2.1.0.3.2).

Additional requirements for the design of the EPR containment include the capability to withstand hydrogen deflagration, allowance of a grace period of at least 12 hours before the need to activate heat removal systems in the event of severe accidents (RRC-B), no paths for direct leakage from the containment into the environment, removal of decay heat from the containment without requiring decompression of the building, and practical elimination of accident sequences with core meltdown involving containment bypass.

Performance of individual components is well presented, and the requirements on their qualification are specified. Information still missing is addressed in Chapter 1.I.

According to the document EDF-SEPTEN 22.02.2003 « Demarche de dimensionnement des ouvrages EPR vis-s-vis du risque lie aux chutes d avions civils » EPR is designed against an air crash of a plane of general aviation so that the consequences at the exclusion area boundary shall not exceed those for DBAs, while the crash of an airliner has very low probability and could be neglected. However, in view of possible human action similar to 11 September suicide attacks, the design of EPR has taken such a possibility into account. The documentation states that the consequences in such a case shall not exceed those of other severe accidents (RRC-B class events).

**4.64 The safety report shall document the safety assessment with sufficient scope and detail to support the conclusions reached. The safety report shall include:**

**(a) A justification for the selection of anticipated operational occurrences and accident conditions addressed in the analysis;**

**(b) An overview and necessary details of the collection of data, the modelling, the computer codes and the assumptions made;**

**(c) Criteria used for the evaluation of the modelling results;**

**(d) Results .of the analysis addressing the performance of the facility or activity, incurred risks and a discussion of the underlying uncertainties; and**

**(e) Conclusions on the acceptability of the level of safety achieved and the identification of necessary improvements and additional measures.**

Review Results

The Requirement is addressed. The document includes anticipated operational occurrences and accident conditions following the guidance provided in EUR requirements. The events are divided into Plant Condition Categories PCC, accidents involving multiple failures (Reduction Risk Category A (RCC–A). and severe accident scenarios with core melt, RRC-B). Each PCC corresponds to a range of estimated occurrence frequencies as follows: PCC1: - all normal operating conditions, PCC2: - all design basis transients, PCC3: - all design basis incidents, PCC4: - all design basis accidents (1.E.5.2.1).

In each of these categories a full spectrum of events is considered, but the guillotine break of the largest pipe in the RCS is excluded by application of the break preclusion principle. Thus the limiting design basis accident is the guillotine break of the largest pipe work connected to the RCS, i.e. the fracture of the surge line or a SIS cold leg injection line. (It should be mentioned, however, that the guillotine break of the largest RCS pipe is considered within the envelope of conditions for which the containment is designed.)

The principal requirements for application of the break preclusion concept are given in section 2E.2.3 ‘break preclusion on main reactor coolant lines’, 3.1 requirements relating to the demonstration of break preclusion. The document states, that demonstrating break preclusion relates exclusively to the first two levels of prevention, namely making a failure highly improbable, and keeping the system within its normal operating constraints through the availability of protective devices (valves, etc.) and in-service surveillance (including in-service inspection) to detect any variation relative to normal operation (loss of integrity, for example).

The non-destructive tests will be qualified in accordance with related regulatory texts. The section 5.4 ‘Inspection Techniques and Procedures’ speaks about NDT, and mentions ultrasonic inspection but no details are given. In particular, there is no discussion of possible manufacturing errors or errors during the plant operation. Further work on this issue is planned (2.E.2.5.2). Also Chapter 1-I on outstanding information includes confirmation that in the next stage it is necessary to perform a comparison between EPR criteria for Break Preclusion and the UK approach for demonstrating incredibility of failure of pressurized components.

The next step safety report should present the break preclusion concept in detail, demonstrate that it can be reliably implemented according to the design, discuss possible failures in the manufacturing of plant elements and in future operation which can adversely influence the effectiveness of break preclusion measures, and justify reliance of the designers on this approach.

Further elements to be included in the next step safety report are listed in Chapter 1.I on identification of outstanding information.

An overview of the collection of data, the modelling, and the assumptions made are given in the chapters on design basis accidents (2P for PCC and 2S for RCC-A and -B).

The codes used for the thermal-hydraulic and neutron design are named [DCD Ch.D1, Tab.2; DCD Ch.D4 4.3]. No comparisons are presented between SMART code calculations and operational or experimental data at high burn-ups. Several thermal-hydraulic and neutron data will be tested in an Initial Test Program [DCD Vol. 2 D2, D3, D4, D5]. For the Level 2 PSA the code MAAP was used [DCD Ch. R 2.2]. The objectives, the experiments and the codes developed and used for sequences with core melt and the behaviour of mitigating measures are described [DCD Ch. S 2.4].

Criteria used for the evaluation of the modelling results are provided in the Chapter 1.E - Safety Principles and Criteria

The results of the analysis addressing the performance of the facility, and incurred risks are presented in the sections on accident analyses, 2.P and 2.S. The probabilistic calculations are given in section 2.R.

Reliability data are derived mainly from operational feedback from France and Germany, supplemented by the EG&G generic reliability database. Reliability data used for instrumentation and control systems are defined in Section R.1.2.2. In general, data is chosen based on the existing French or German design that most closely matches the EPR. In case of equivalent data from different sources, the most conservative data are used. With regard to components whose design is not yet precisely defined or which are not used in French or German plants, reliability data is taken from the EG&G database.

The break preclusion concept is in agreement with the laws in force and with the actual practice in France and Germany, but not necessarily in other countries. The demonstration of the reliability of break preclusion concept should be presented in more detail than that given in the documentation. Since one of the two pillars supporting this concept is in service inspection, and since the difficulties occurring in Olkiluoto were related to the future realisation of the ISI programme, the documentation states that the ISI programme will be defined during the design stage on the basis of the mechanical analysis results (fatigue, sudden break, etc,) and on feedback relating to operation in certain areas (mechanical problems, for example).