

**IAEA Generic Review for UK HSE of New Reactor Designs against  
IAEA Safety Standards  
ESBWR**

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

## 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. Following the standard DCD format of the US NRC a safety analysis has been performed to determine whether the design and engineered safety features fulfil the safety functions required of them. Detailed information is provided on how the safety objectives and criteria established by the US NRC and the UK HSE are addressed. It is stated that as much as possible the ESBWR builds on the design features of operating BWRs.

The results of the accident analyses are provided in Chapter 15 of the DCD. The analysis follows the standard US NRC procedure based on a classification of plant conditions. The analyses cover normal operation, anticipated operational events, infrequent events, design basis accidents, special events and beyond design basis accidents.

Both deterministic and probabilistic analyses are performed with the objective to demonstrate that an adequate level of safety has been achieved.

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”. A special feature is aimed at arresting a molten core by the innovative Basemat Internal Melt Arrest and Coolability Device (BiMAC). Little information is available in the submission on the functioning of the BiMAC. On the basis of what has been provided in the submission it appears that it has been developed to the concept stage only.

**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 Head document makes reference to the extensive experience of operating BWRs and the maturity of the design by documenting the various stages of the evolution of the design. DCD Chapter 1.9 systematically addresses compliance with US NRC Regulatory Guides and the Industrial Standards.

GE has developed the Nuclear Safety Operational Analysis (NSOA) as a systematic qualitative approach that shows which protective functions and systems are required to show compliance with US NRC criteria for events addressed in the safety analyses. Results of the accident analyses are provided in DCD Chapter 15.

The innovative passive safety features are described. Reference is made to documentation related to the verification of the assessments by experimental results. The performance of the innovative passive safety features needs to be reviewed at the next step. Particular attention has to be paid to the scaling of test results. Very limited information only is available on the concept of the BiMAC.

Reference is made to a PSA, which, however, is not included in the documentation. Due to the use of passive safety features the PSA results show very low numbers for the frequency of severe accidents. The PSA will have to be reviewed at the next stage. In particular, attention will have to be given to the very low frequencies claimed for severe accidents. Detailed information on the functioning of the BiMAC is not yet available. It will strongly influence the results of the Level 2 PSA.

**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 was requested. However, the Head Document is accompanied by the DCD document following the standard NRC procedure for detailed safety analyses commensurate with the potential radiation risk arising from an NPP. However, some parts of the detailed analyses are not yet available.

## 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. Radiation protection requirements for workers and the public for normal operation and accident conditions are addressed. The analyses and the documentation submitted follow the US NRC procedure and are documented in the standard DCD format. This is preceded by the Preliminary Safety Report following the structure of the UK HSE request. It provides precise guidance on where the relevant information is found in the DCD.

Explicit reference is made to the safety objectives and criteria established by the US NRC and the UK HSE. Table 2.2-1 provides a comparison of US and UK radiation exposure goals for normal operation and accident conditions. It is recognised that the SAP NT.1 Numerical Targets and Legal Limits “do not precisely line up against the US basis”. It is indicated that a specific UK compatible assessment will be performed at a later date in the review process.

GE has developed the Nuclear Safety Operational Analysis (NSOA) as a systematic qualitative approach that shows which protective functions and systems are required to show compliance with US NRC criteria for events addressed in safety analyses. Table 15.0-1 of DCD Chapter 15 provides an abnormal event classification scheme matrix for AOOs (considered part of normal operation), Infrequent Events, Accidents and Special Events. The DCD Chapter 15 provides the results of the accident analyses.

The conclusions of the probabilistic analyses are summarized in Chapter 19 of the DCD on “Probabilistic Risk Assessment and Severe Accidents”. Reference is made to the Topical Licensing Report NEDO-33201 Revision 2 April 2007. It is claimed that a “full scope (Level 1, 2, and 3) PRA, that covers both internal and external events, for at-power and shutdown operations has been performed”. However, Chapter 19.2.3.1.2 states that a bounding rather than best estimate method is used for assessing containment performance. For this purpose the Risk Oriented Accident Analysis Methodology (ROOAM) has been developed. The results of the PSA demonstrating compliance with the US NRC goals by large margins are given in Table 2.6-3.

Severe Accident Preventive and Mitigative Features are briefly addressed in DCD Chapter 19.3.1 and 19.3.2. Little information is presented on the functioning of the innovative Basemat Internal Melt Arrest and Coolability Device (BiMAC) (DCD Chapter 19.3.2.6).

The ESBWR design is undergoing the design certification process of the US NRC. The report indicates that Final Design Approval is expected in late 2008 and Design Certification in late 2009. The report also makes reference to the experience in licensing the BWRs and ABWRs in foreign countries.

The accident analyses follow US NRC categories and methodology, which are not exactly consistent with the UK NII or the IAEA categories. As indicated analyses better conforming to the UK NII categories will be presented in the next step. The ESBWR design includes features specifically addressing a selection of specified accidents beyond the design basis, including selected severe accidents, as requested by IAEA NS-R-1. Best estimate analysis could be used for PSA and analyses of the specified accidents beyond the design basis rather than bounding assumptions. More information would be necessary regarding severe accident assessment. The report states that detailed PSA information can be obtained from the Topical Licensing Report referred to above.

**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 limits specified by the SAPs of the UK HSE, which also reflect the IAEA BSS.

The methodology for estimating annual occupational radiation exposure is described in DCD 12.4. The results based on this methodology are provided in Table DCD 12.4-1. In comparison with past and present actual data, the methodology is found to be conservative. ALARA related cost-benefit assessments are reported in 2.2.3.5. No specific probabilistic evaluation of worker risk of death is available. Rather the accidental exposure of workers is benchmarked against the probability of core damage.

The method for calculating public radiation exposure from normal operation is detailed in DCD Chapter 12.2 and summarized in Table 2.2-1. It is stated that in the US the ALARA considerations are satisfied if the acceptable dose limits are met as specified in 10 CFR 50 Appendix I. For accidental releases within the design basis the results of DCD Chapter 15 are summarized in Table 2.2-2. SAMDA assessments are presented to demonstrate that the ALARA principle has also been applied to severe accidents. Reference is made to the GE Licensing Topical Report, ESBWR Severe Accident Mitigation Design Alternatives (August 2007).

Regarding the use of SAMDA it is noted that the IAEA Safety Standards do not include such an approach; rather the term risk is used as a multi-attribute quantity and the use of the expectation value for widely differing consequences is avoided (see also Glossary of the BSS, Glossary of safety terms edition 2007).

**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. This safety assessment Requirement is complemented by the more detailed principle technical Requirements in Chapter 4 and by the Requirements for plant design as provided for by NS-R-1. Information on how this Requirement has been addressed is provided in Chapter 15 of the DCD following standard US NRC procedures. This specific procedure is also applied to the calculation of radiological consequences. The summaries in Chapter 2.2.3 and 2.2.4 provide some information on how the US NRC requirements relate to the UK HSE. It is indicated that specific UK compatible assessments will be provided later.

Though more detailed the SAP probability categories are consistent with the categories of IAEA Requirements. It is suggested that for the next stage of the review more detailed information consistent with the IAEA or the SAP categories be provided.

**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 ESBWR is an evolutionary design. It is stated that as much as possible the ESBWR builds on the design features of operating BWRs. A main difference is the taller reactor vessel with the addition of a partitioned chimney above the core and a corresponding taller downcomer annulus. Another design principle was the use of passive safety features including the Gravity –Driven Cooling System (GDCCS), the Automatic Depressurisation System (ADS), and the Passive Containment Cooling System (PCCS).

DCD Chapter 1.9 systematically addresses conformance with the applicability of US codes and standards including NRC Regulatory Guides, Industrial Codes and Standards, Action Plan Items, Generic Issues and US URD requirements.

DCD Chapter 15 presents results of the accident analyses to determine whether the design and engineered safety features fulfil the safety functions required of them. Subchapter 15.1 describes the results of the Nuclear Safety Operational Analysis (NSOA). This system level qualitative FMEA methodology is used to systematically obtain event paths constituting the minimum required actions to bring the plant to a stable shutdown condition for each event (Figures 15.1-1 to 15.1-47). Table 15.1-3 gives the list of events and applicable plant operating modes which are then analysed. This includes waste gas system leaks or failure. The analyses make use of the TRACG computer code. The application of the code and the related test and analysis program is summarized in Subchapter 1.5.2.1. The accident analyses include an assessment of the radiological consequences in accordance with US NRC requirements. As a conservative approach to containment performance major core degradation and melting is assumed though the analyses show that core integrity is maintained.

Severe accidents with core degradation and melting are addressed by provision for flooding and cooling of the reactor pressure vessel from the outside. If this should not be successful, RPV melt-through accidents will be mitigated by the Basemat Internal Melt Arrest and Coolability Device (BiMAC). Very limited conceptual information is included in DCD Subchapter 19.3.2.6. It is stated in subchapter 19A.8.4.6 that it “has been developed to a conceptual level, with several design details that are not yet finalized”. These safety features respond to the NS R-1 Requirement to address in the design specified accidents beyond the design basis, including selected severe accidents.

In DCD Subchapter 19.2 it is claimed that the ESBWR PRA is a “full-scope (Level 1, 2, 3) PRA that covers both internal and external events, for at-power and shutdown conditions”. The PSA (Reference is provided) is not included in the documentation.

DCD Chapter 19 gives a short summary of PSA Level 1 results. Regarding Level 2 aspects it is reported that the ‘Risk Oriented Accident Analysis Methodology (ROAAM) has been developed. Uncertainties in parameters and scenarios challenging the containment that cannot be reasonably quantified are treated conservatively, rather than using best estimate methods.

Potential Large Release Sequences and containment performance are summarized. Consequence calculations from internal events are included in the Head Document in Figure 2.6-2. DCD Subchapter 19.6 concludes that the US NRC requirements and safety goals are met.

Since the PSA is only briefly summarized and not included in the documentation it should be reviewed in detail at the next step. It is noted that the CDF from internal events at power ( $1.2 \text{ E-8}$ ), at shutdown states ( $8.8 \text{ E-9}$ ) and internal events LRF (in the range of  $1.0 \text{ E-9}$ ) is very low. Level 2 and 3 PSA results will strongly depend on the performance of the BiMAC, which is in the state of a conceptual design only.

It is good practice to use best estimate analysis in PSAs.

**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 partially addressed. Individual and societal radiation risks are calculated in accordance with the procedures of the US NRC for normal operation (DCD Chapter 12.2) and accidents within the design basis (DCD Chapter 15, Table 2.2-2). The summaries in Chapter 2.2.3 and 2.2.4 provide some information on how the US NRC requirements relate to the SAPs of the UK HSE. UK compatible assessments will be provided later. Severe accidents are addressed in Chapter 2.6. The calculations of individual radiation risk follow standard US NRC procedures.

Since the site for the plant is not known, detailed assessments addressing this Requirement will have to be performed at the next step.

**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 partially addressed. A more detailed evaluation of the radiation risks posed by the facility is given in Requirement 4.19. Efforts to minimise radioactive waste are briefly described in the head document. Novel design features have been added to the design with the aim of significantly reducing the probability of severe accidents with potential long-term impacts. SAMDA assessments are presented to demonstrate that the ALARA principle has also been applied to severe accidents.

**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 through adherence to the many requirements and guidelines representing the defence-in-depth concept. As demonstrated by the accident analyses a combination of several layers of protection is present throughout the design. The design includes innovative features, in particular passive safety features including the BiMAC to arrest a molten core strengthening the 4<sup>th</sup> level of defence-in-depth. On the other hand this results in the fact that some standard active features of BWRs have been withdrawn.

The basic safety approach to the safety of the ESBWR is deterministic. It is an evolutionary design making use to the extent possible of design features of operating BWRs. The approach is complemented by probabilistic analyses.

The performance of the innovative passive safety features needs to be evaluated in detail in the next step. A more detailed assessment of defence in depth is provided 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 a safety analysis for events selected by the systematic NSOA method. The documentation in DCD Chapter 15 includes a description of the results of the safety analyses performed for the different initiating events. Details in form of diagrams of the thermal hydraulic analyses are provided. The basic approach to the safety assessment is deterministic following US NRC procedures.

The deterministic analyses are complemented by PSA Level 1, 2, 3, considerations including shut-down states and external events.

The assessment of the containment performance and the consequence analysis of severe accidents will be influenced by the performance of the BiMAC device, which is in the state of a conceptual design only.

The analysis of accidents beyond the design basis could make use of best estimate analysis methodology as recommended in NS-R-1.

**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 analyses are based on the use of the TRACG computer code. As summarized in DCD Subchapter 1.5.2.1 it is a multi-dimensional two-fluid model for the thermal hydraulics and a three-dimensional neutron kinetics model. TRACG contains a set of models for BWR components. A summary of the test and analysis program is also provided. For more details the Chapter refers to a set of publications. Other computer codes used (e.g. for the PSA) are well referred to in the text. At this stage no information is available regarding the computer codes to be used for modelling of the BiMAC.

At the next step particular attention has to be given to the modelling of the natural circulation.

More details are provided under the assessment of Draft Requirement 4.60.

**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. The Head Document and the DCD Chapter 1 make extensive reference to the development of the ESBWR as a long-term evolutionary process making use of the experience gained. DCD Table 19.2-1 gives a comparison of ESBWR features with existing BWRs. Extensive reference is made to the regulatory and utility requirements addressed. DCD Table 19.2-2 and 19.2-3 lists those features which have been influenced by the results of the PSAs.

The iterative process leading to the ESBWR design is well documented throughout the DCD. Innovative features have been added, in particular the natural circulation within the vessel for power production and the extensive use of passive systems to cope with design basis accidents.

## 4.19 Potential Radiation Risks

**4.19 The potential radiation risks 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. Potential radiation exposure of workers is identified and assessed in DCD Ch. 12, Radiation protection, section 12.4, Dose assessment, dealing with doses during normal operation to be obtained due to maintenance activities in drywell (12.4.1), reactor building (12.4.2), fuel building (12.4.3), turbine building (12.4.4), radwaste building (12,4,5) and due to work at power (12.4.6).

Airborne releases of radioactive materials are considered (12.2.6) as well as liquid releases (12.2.2.3).

The radiation doses to the public due to airborne and liquid releases for normal operational conditions are evaluated (12.2.2.2 and 12.2.2.4).

Radiation risks in case of anticipated operational occurrences and accidents are presented for each accident in a section 15.*n*.4, where *n* is the number assigned to the accident considered.

Chapter 15.2 deals with Analysis of Anticipated Operational Occurrences and demonstrates that AOO do not lead to fuel failures and thus involve no significant radiological consequences (15.2).

Chapter 15.3 deals with Analysis of Infrequent Events, for which there is some release of radioactivity contained in the coolant or in a fuel rod, corresponding at the worst to a small increase in the yearly integrated exposure level. The equipment outside the reactor is also taken into account in (15.3.16).

In the Analysis of Accidents the normal full spectrum of accidents is considered, showing that the most significant consequences can arise in the case of Loss-of-Coolant Accidents in which the release of core inventory to the containment is conservatively assumed, although the thermal hydraulic analysis shows that the fuel would not be damaged in case of LOCA.

Radiation releases and dose rates in NPP rooms are calculated and specified in many detailed tables covering AOOs, IEs and DBAs.

Radiological Consequences at the exclusion area boundary and at the low population zone boundary are determined for this spectrum of accidents. Other design basis accidents including Main Steamline Break Accident Outside Containment, Control Rod Drop Accident, Feedwater Line Break Outside Containment, Small LOCA Outside Containment, RWCU/SDC System Line Failure Outside Containment and Spent Fuel Cask Drop Accident are considered.

Also Special Events including Overpressure Protection, Shutdown without Control Rods, Standby Liquid Control System Capability, Shutdown from Outside Main Control Room, Anticipated Transients without Scram, Station Blackout, Safe Shutdown Fire are considered.

In order to compare the US approach to accidents with the frequency categories used in the UK, the designers have placed AOOs into the  $>1.0 \text{ E-3/year}$  box, IEs into the  $1.0 \text{ E-3}$  to  $1.0 \text{ E-4/year}$  box and DBAs into the  $<1.0 \text{ E-4/year}$  box, and used bounding radiological calculations for comparison to the UK targets and limits (PSAR 2.2.2).

Current ESBWR assessments demonstrate that all Basic Safety Limits (BSLs) are met by a considerable margin, with results close to and sometimes below the Basic Safety Objectives (BSOs) (PSAR, Table 2.2-1).

**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 startup 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” is addressed in sufficient detail [Head Doc. Tab.2.4-1, DCD Ch.4]. This safety function covers operational occurrences up to accidents. 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. 16, B3.1.1]. Two redundant Remote Shutdown panels are available [Head Doc. 2.5.3.4.3, DCD 7.4.2].

The safety function ‘Heat Removal from the Core’ is carried out by passive systems – no AC power is needed. Therefore, the ESBWR does not have the traditional RHR system. Active human action is required only after 72 hrs [Head Doc. 2.12.1; DCD Ch. 19A.3.1].

It is claimed that the safety function” Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases” is met and the release values are well below required limits [Head Doc. 2.6.6.2, Tab. 2.6-3] for internal events as well as for external hazards.

It should be clarified how the third safety function can be met during some shutdown stages with open containment .Novel features are the natural circulation in the vessel and the decay heat removal from the core and the containment. These features should be checked in more detail at a later stage.

Based on the three fundamental safety functions, the plant specific safety functions have been derived and are listed comprehensively in DCD 3.2. This is the basis for the identification and classification of the SSCs which follows the 10 CFR 50. All classified systems and related classification requirements are set out in dedicated tables (Table 3.2.1).

**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

The Requirement is addressed. The ESBWR natural circulation and the passive safety systems are significantly simpler than typical BWR safety systems since they contain significantly fewer components. This reduces the required tests, inspection and maintenance. They require no active support systems, and their readiness is easily monitored. 3 out of 4 Isolation Condenser System sub-loops are adequate operating alone to remove residual heat from the reactor core and assure that fuel and Reactor Coolant Pressure Boundary design limits are not exceeded [DCD 3.1.4.5]. The single failure criterion is considered –active or passive for electrical systems and active for Design Bases Events. Common Cause Failures are considered [DCD Ch.15 A.2 and A.3; DCD Ch.15 Tab. 15 A-1]. It is claimed that redundancies implemented, passive safety systems which need no AC power to operate and rigid QA procedures reduce the reactor core damage frequency and severe accident risk [Head Doc. Tab.2.6-1, DCD Ch. 19]. An evaluation of the principal design criteria as measured against the USNRC General Design Criteria for NPPs is outlined in detail [DCD Ch. 3.1], this includes e.g. redundancies, diversities, separations, the quality of components, planned inspections and testing; it is claimed that the criteria are met. An extensive QA programme is available [DCD Ch. 17].

More details should be presented for shutdown stages. The methodology of how Common Cause Failures are calculated should be outlined in more detail.

## 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, generic site considerations and the methodology for site-specific assessments could be addressed only.

(a) The physical and chemical characteristics that will affect the dispersion or migration of radioactive material through direct and indirect pathways are not discussed. However, it is understood that it is a very site-specific issue. Normal practices and efforts to demonstrate compliance with HSE requirements will address this topic for a selected UK site.

(b) This is addressed. Table 2.7-1 of the ESBWR UK Preliminary Safety Report lists the envelope site parameters for ESBWR. If the site-specific parameters fall within the envelope, the site is considered suitable for locating the ESBWR. Section 2.7.2.4 of ESBWR UK Preliminary Safety Report describes the external natural and human induced hazards considered in the siting of the ESBWR. Evaluation of hazards from nearby industrial and military facilities for a chosen ESBWR site is described in Section 2.2 of the Design Control Document.

The ESBWR is designed to an envelope of two ground motions: 0.30g peak ground acceleration anchored to USNRC R.G. 1.60 ground motion spectrum and 0.5g pga anchored to the North Anna site specific ground motion spectrum; this is well above the IAEA minimum of 0.10g peak ground acceleration for SSE. ESBWR is designed to envelop response from a variety of site conditions (i.e., uniform soft, medium and hard soil, layered sites and North Anna specific). It is expected that any selected future site be covered by these site conditions. This follows the traditional practice in the siting of standard plants

c) Individual and societal risk goals have been met for the US design. Section 2.7.2.3 describes this assessment. It is proposed by the vendor that UK Government siting policy will be reviewed for the specific UK site.

The documents reviewed contain sufficient detail and relevant information (ESBWR UK Preliminary Safety Report and Design Control Document) to allow assessment of whether the subject Requirement is addressed.

**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 para. 5.10).**

#### Review Results

The Requirement is addressed. Since the assessment is very specific to the site selected the procedures and methodologies for site assessment can be addressed at this stage only. The procedures for selecting the site and identification of hazards included in the documentation 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).

A combination of deterministic and probabilistic criteria is used in the site assessment. Earthquake, external flooding and tornado parameters are chosen for the standard design to essentially cover all potential US sites (except California) and are expected to envelope all UK sites. Selection of design basis human-induced hazards is done using a probabilistic threshold.

Table 2.6-2 of the Preliminary Safety Report shows that the core damage frequency from internal and selected external events is estimated as  $6E-08$  per reactor-year. The CDF contribution from natural and human-induced hazards can only be evaluated using site-specific data.

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

The documents reviewed contain sufficient detail and relevant information (ESBWR UK Preliminary Safety Report and Design Control Document) to allow assessing if the subject Requirement is addressed.

## 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. The ESBWR can make use of the experience with the ABWRs. The PSAR Chapter 2.2.3.1 describes that the radiation exposure of working personnel in normal operation has been decreased due to improvements in plant operation and projected lower forced outage rates. In particular design improvements and simplifications should further reduce occupational exposure. ESBWR design focuses on alloy selection (e.g. cobalt elimination) and water chemistry modifications and control to minimize radioactive nuclide build up (PSAR 2.2.3.2). Separation of clean and controlled access areas and reduction in the plant personnel radiation exposure is achieved by (1) minimizing the necessity for and amount of personnel time spent in radiation areas and (2) minimizing radiation levels in routinely occupied plant areas in the vicinity of plant equipment expected to require personnel attention (PSAR 2.2.3.3).

Under accident conditions exposure of workers is limited due to layout and shielding considerations. It is shown that the only permanently manned onsite location after accidents is the control room, where the calculated exposure of workers after postulated DBA LOCA is limited to 41 mSv which is a decade below the UK BSL of 500 mSv (DCD 15.4).

As described in Chapter 6, a number of engineered safety features are aimed at limiting the exposure of the public in case of accidents. These include the containment, containment passive cooling system, combustible gas control within the containment, system of fracture prevention of primary cooling system pressure boundary, emergency core cooling systems etc.

The likelihood of events that might lead to reactor core damage is very low and the DCD Section 2.6 shows that it is estimated to be  $6 \times 10^{-8}$ /reactor-year from all events (internal and external), two decades below the INSAG targets referred to in the IAEA Safety Standards. This is explained by the basic simplicity of the direct cycle BWR with many diverse and redundant ways to add water to the RPV and also by the simplicity, diversity and redundancy, incorporated in the ESBWR Design.

Mitigation of consequences of accidents has been addressed by several safety features designed to protect integrity of reactor pressure vessel and containment even in the case of a severe accident, as described in PSAR Chapter 2.12. They include in particular the Gravity Driven Cooling System, Automatic Depressurisation System (ADS) with safety valves and depressurization valves, Passive Containment Cooling System (PCCS) with vacuum breakers, and the natural circulation system in the reactor core.

However, there is no clear presentation of radiological results of severe accidents, nor of the scenario leading to core melt and containment failure. The section on special events shows that all scenarios considered there are successfully terminated without core melt. Thus, while the frequency of large release is given, and is shown to be very low, there is lack of

information on which plant failures could result in severe accidents and which doses would be estimated.

Concerning Principle 8, that “all practical efforts must be made to prevent and mitigate nuclear or radiation accidents”, the issue of further possible mitigation of severe accident consequences has been studied as described in the section on Severe Accident Mitigation Design Alternatives (SAMDA) presented in 2.2-6. A further discussion on the SAMDA approach is given in the assessment of IAEA Draft Requirement 4.45.

The documentation claims that the ESBWR meets the goals of US NRC and UK NII by a large margin.

The scope of radiation protection studies includes other phases of the plant life cycle, including radwaste management and plant decommissioning. Several measures have been taken specifically to reduce radiation doses during decommissioning.

Significant steps have been taken to increase the level of safety of the ESBWR in comparison to conventional designs. The advantages, potential draw-backs and additional needs for analysis are 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 occupational radiation exposures have been reduced in BWRs so that in 2004, the average annual US power reactor exposures were 1560 man-mSv (156 man-rem) per reactor at BWRs (per reference 2.2-3). The ESBWR combines advanced facility design features and administrative procedures designed to keep the occupational radiation exposure to personnel as low as reasonably achievable (ALARA). During the design phase, layout, shielding, ventilation and monitoring instrument designs are integrated with traffic, security and access control.

Improvements to the plant design to reduce radiation exposure to workers have been based on feedback from operations of the existing BWR fleet, as well as technology improvements in materials, simplification of systems needing maintenance, etc.

The assessment if further reasonable measures could be taken to reduce operator dose was based on a cost-benefit analysis. The benchmarks taken in the documentation are based on the HSE paper "Tolerability" (reference 2.2-4) and resulting cost-benefit analysis. It is considered conservative, because it is based on the linear theory of radiation exposure risk.

In case of population, the conservative analysis performed for UK ESBWR found that averting exposure was costed at \$2000/man-rem, which is double the minimum US regulatory requirement. The Requesting Party has not found any design alternatives that could be done within the corresponding budget.

The assessment provided in the documentation covers the whole field of normal operation and accidents, including workers and public exposures. Although the method of cost-benefit analysis with its monetary characteristics is not used by the IAEA, nevertheless the intent of Requirement 4.25 has been addressed, though in a way differing from that of the IAEA.

**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. Public radiation exposure has been determined for all events leading to radioactive releases and has been shown to be smaller than the design acceptance criteria of both the UK and the US licensing processes (DCD Table 15.4-9, Table 2.2-1). The analyses include normal operation conditions and events of various frequencies, starting with Anticipated Operational Occurrences, expected to occur once in the lifetime of the reactor, Infrequent Events expected to occur with the frequency of 1 E-2 to 1 E-4 per reactor-year, and Design Basis Accidents, expected to occur with the frequency less than 10<sup>-4</sup> per reactor year. Radiological protection provisions are described for each of these states of the plant. Their effectiveness is evaluated on the basis of calculations, validated by operational experience and specific experiments. Scenarios of various accidents are also provided (Chapter 6, Tables 6.3.7 to 6.3.10).

Scenarios of severe accidents are not described. The next step safety report should provide these descriptions with demonstration of their very low frequency.

## 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 DCD shows that most of ESBWR structures, systems and components are of proven design, while a number of safety features are of novel design. Most components in the ESBWR are standard BWR components that have been operating in the field for years (steam separators, control rods and guide tubes, core support structure, etc.). Standard systems are used where practical. Many features are common to ABWR – vessel type, fine motion control rod drives, pressure suppression containment, fuel designs, materials and water chemistry (PSR 2.1.2). The size of the pressure vessel with the chimney above the core is larger than the size of previous BWR pressure vessels and thus requires further consideration.

The range of data is extended to ESBWR parameters, e.g. separators, large channel two-phase flow, and isolation condensers. Squib and deluge valves in Gravity-Driven Cooling System (GDCCS) are based on the experience of many BWRs (PSR 2.12.2). SRVs are similar to those used in all current BWRs (PSR 2.12.3).

The ESBWR containment is similar in construction to the ABWR, but with an elevated suppression pool and a slightly larger volume to accommodate the passive ECCS (PSR 2.1.1.2).

The main difference consists in that ESBWR relies on natural circulation to provide heat removal from the core, and also uses natural circulation in ECCS. This should be considered as a novel feature, even if the elements are proven. The ESBWR design reduces the frequency and consequences of large loss of coolant accidents (LOCA) by removing the recirculation system altogether.

In case of novel features there are extensive databases available, and test programmes have been conducted. The DCD claims that the pertinent operational experience is positive. However, consideration of the past operational experience should be outlined in more detail and the measures taken to prevent recurrence of past difficulties should be presented (e.g. the issue of control rod removal). The ESBWR design addresses generic safety issues from NUREG-0933 as shown in DCD Tables 1.11-1 and 1A-1 and considers requirements from various NRC Generic Letters and Bulletins (see DCD Tables 1C-1 and 1C-2) that are based on the operating experience of existing plants (DCD 2.4.1). Since generic safety issues and NRC generic letters reflect relevant operational experience, including results of root cause analysis of anticipated operational occurrences and accidents where appropriate, Requirement 4.27 is addressed.

**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. Defence in depth is enhanced. Multiple barriers exist and in comparison to previous BWRs they are strengthened. For example, the intersystem LOCA issue is resolved by strengthening low pressure piping interfacing with RCPB. Fission products, hydrogen, oxygen are contained in a low leakage containment. The issue of defence in depth is reviewed in more detail in the assessment of IAEA Draft Requirement 4.45.

Fire protection for ESBWR uses the concept of defence in depth to prevent fires from starting, to rapidly detect, control, extinguish those fires that do occur, and to provide protection for structures, systems and components important to safety so that the fire does not prevent safe shutdown of the plant (DCD 9.5.1.1).

Requirements of redundancy, separation, independence of redundant systems, resistance to single failure and diversity are addressed and qualitative characteristics are presented showing how these concepts are satisfied. All safety related systems are composed of four divisions (GDCS - PSR 1.12.2) provided with physically separated and electrically independent batteries (NRC General Design Criterion 17, DCD). Redundant divisions are physically separate DCD 8.1.5.2.1, Crit. 22, DCD 3.4.1.3. The Reactor Protection System is separated from process control systems (Crit. 24, DCD). The single failure criterion is addressed (Crit. 24, 25).

Passive features are an important part of ESBWR design principles. The short-term and long-term Gravity-Driven Cooling Systems (GDCS) provide cooling water under force of gravity to replace RPV water inventory lost during a postulated LOCA and subsequent decay heat boil-off (PSR 2.12.2). The deluge lines connecting GDCS pool to the lower drywell do not require the actuation of squib actuated valves on the GDCS injection lines to perform their functions (PSR 2.12.2). Temperature and pressure in the containment vessel are limited by using Passive Containment Cooling System (Crit. 16, DCD 6.2 Containment systems). To assure availability, no valves are employed (Crit 38, DCD 3.1)

Safety margins are increased in comparison to previous BWR designs (DCD 3.1). It is estimated that the ESBWR containment has a higher factor of safety than earlier BWRs (PSR 2.6.4.2). Intersystem LOCA issue is addressed by providing the low pressure piping systems that interface with RCPB with strength sufficient to withstand 0.4 times the normal design RCPB pressure (ESBWR DCD, Tier 2, Ch. 3, App. 3K). Diversity is applied e.g. in squib valves (PSR 2.12.2) and ADS-SRV valves (PSR 2.12.3).

A negative void reactivity coefficient is assured. The reactor core and associated coolant system are designed so that in the power operating range, prompt inherent dynamic behaviour compensates for any rapid increase in reactivity in accordance with Crit.11 (DCD 3.1). The

control rod drive mechanical design incorporates a passive brake and hydraulic inlet check valve that prevent rapid rod ejection (Crit. 28, DCD 3.1)

More details should be included in the next step report on the added Basemat-Internal Melt Arrest and Coolability device (BiMAC).

Also, DCD 3.1 claims that “the containment integrity is assured for postulated accidents”(Crit. 41, DCD 3.1). No evidence is provided that the issue is resolved

**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, and complemented by a subsequent programme of monitoring during operation.**

#### Review Results

The Requirement is addressed. Innovative improvements incorporated in the design are described as thoroughly tested, or developed in such a way, that the new design eliminates existing components or systems and thus eliminates related safety issues.

In the design of ESBWR the jet pumps and the external recirculation systems, with all their pumps, valves, piping, and snubbers have been eliminated (PSR 2.1.1). This has been possible due to installation of shorter fuel elements and adding a chimney above the core which provides an additional driving head for natural circulation flow through the core (PSR 2.12.5). The data base, experiments in various facilities and operating experience for establishing hydrodynamics, stability performance and checking computer codes is described (PSR 2.12.5). The chimney study testing program has been successfully completed (DCD App. 3L.3, NRC General Design Criterion 12).

Although depressurization valves, wet well drywell vacuum breakers and isolation condenser heat exchangers are based on those previously used in BWRs (PSR 2.1.2), due to their size and thrust loads they have undergone full engineering testing including full size prototypes (PSR 2.12.3, PSR 2.12.4).

There have been extensive qualification tests of the PCCS, including full-scale component tests and full height scaled integral tests (PSR 2.12.4).

Regarding the issue of thermal hydraulic power oscillations, operating experience has shown large BWRs to be inherently stable against xenon induced power instability. Negative reactivity coefficients also assure good load following and strong damping of spatial power distribution (DCD 3.1). Thermal hydraulic power oscillations were a problem in BWRs, e.g. La Salle 1988, KKI-1 1991, KWW 1992, also minor oscillations in Sweden and Spain. Automatic insertion of selected control rods in case of instability conditions was proposed in several reactors to avoid entry into unstable range (Japan, Spain, and Sweden). No evidence is provided on how this issue has been resolved; however, the RP claims a large margin to instability for ESBWR. The issue should be addressed in more detail in the next review steps.

Regarding the issue of vibrations, the ESBWR design relies on proven components to avoid new vibration issues. Since it is a natural circulation plant where no recirculation motors exist there is no source of flow excitation due to the pumps vanes. However, a flow-induced vibration (FIV) testing program of the reactor internal components of the ESBWR prototype plant is to be completed to demonstrate that the ESBWR internals design can safely withstand expected FIV forces for reactor operating conditions up to and including 100% power and core flow (DCD App. 3L). The second phase of the program is focused on preparing and performing the startup test program that will demonstrate through instrumentation and inspection that no FIV problems exist.

The ESBWR will use a steam dryer design patterned after the new steam dryer design developed for BWR operating plants. The testing program already performed is presented, and the detailed program that is planned is described in DCD Section 3L.4.

**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 regarding seismic, system quality group and safety are well described [DCD Ch.3.2 and table 3.2.1] as well as event classification and acceptance criteria [Head Doc. 2.5 and table 2.5-1-5, DCD 15.0.1-3]; for each event the causes are identified, the sequence of events and the system operations are evaluated, the results given, the barrier performance discussed and the radiological consequences evaluated. Its importance for safety is considered; probabilistic considerations and frequencies are used to group events. The links between SSC and the systems should be outlined in more detail. Also, all the software of the safety-classified programmable I&C should be outlined in more detail.

The classification follows the standard US procedure and thus does not explicitly address the relevant Requirements as formulated in NS-R-1, which are consistent with the formulation of the principles of the UK HSE SAPs. Therefore, there is the need in the next step to review in detail to which extent the classification system used for the ESBWR is implicitly addressing the IAEA Requirements and the SAPs.

It is claimed that all relevant regulatory requirements and industry codes and standards are met and all relevant codes have been used [Head Doc. 2.3, 2.4 and Tab. 2.4-1, DCD Ch. 7.1.6 and tab. 7.1-1 and 8.1.6 and tab.8.1-1].

It should be evaluated in detail to which extent national (US) codes (mainly industry codes) and requirements comply with UK requirements.

**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. Section 2.7.2.4 of ESBWR UK Preliminary Safety Report describes the external natural and human induced hazards considered in the siting of the ESBWR. Evaluation of hazards from nearby industrial and military facilities for a chosen ESBWR site is described in Section 2.2 of the DCD.

A combination of deterministic and probabilistic criteria is used in the site assessment. Earthquake, external flooding and tornado parameters are chosen for the standard design to essentially cover all potential US sites (except California) and are expected to envelope all UK sites.

Selection of design basis human-induced hazards is done using a probabilistic threshold of  $1E-07$  per year. The procedures for selecting the design basis external hazards are described in Section 2.7.

Section 19 of the DCD describes the PSA based Seismic Margin Assessment performed to demonstrate a margin of 1.67 over the SSE for the Standard Plant. This demonstrates the capability of an ESBWR plant to withstand beyond design basis earthquakes.

Section 2.7.2.4.4 states that impacts from adjacent sites and malicious threats to the plant will be examined in detail during the next phase for the particular plant site.

The documentation provided the relevant information to allow assessing if the subject Requirement has been addressed.

**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. Internal hazards such as pipe breaks, internal flooding and spraying, internal missiles, load drop, internal explosions and fire are addressed in Section 3.5.1 of DCD. The layout of the plant will be such as to minimize the risk from turbine missiles to impact safety significant components. Further, measures have been taken aimed at a low turbine disk breakup probability.

Procedures for design against postulated loads and load combinations are described in Section 3.8 of the Design Control Document.

The documentation provided the relevant information to allow assessing if the subject Requirement has been addressed.

**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 ESBWR design for the RCS follows the ASME III -code and, hence, selection and application of materials are also in line with this code. Hence, due attention is paid to the behaviour of material under transient and accident conditions.

The mechanical design and the material selection follow established international codes and standards, but some major improvements of the past (such as LBB) do not seem to have been incorporated.

The mechanical / material aspects are addressed in the documentation; however, some important present day advances might have been missed.

The ESBWR fuel is described in Chapter 4. The description lacks detail on materials used for fuel rods, cladding and control rods. Fuel is, however, stated as of the same composition as the NRC-licensed fuel GE-14. Hence, it is anticipated that it will meet the relevant criteria. This should be confirmed for the UK application case.

Furthermore, should the removal (by design) of the control rod drop accident from the list of postulated initiating events not be justified, this event should then be reassessed in order to demonstrate that the RIA safety limits are met for fresh and irradiated fuel.

In the next step the RCS design should be further assessed with respect to the number of welds, sort material (preference no moulding), reduction of irradiation of material in the belt line, and LBB-behaviour (pipe whip restraints remove safety concerns of LBLOCA, but increase radiation dose to workers, as their dismantling for inspection of RCS-piping and recomposition after that takes much time and, hence, cause radiation dose).

High burn-up has special considerations: RIA<sup>[1]</sup>-limits are not well-known, as are 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%). In nuclear design, the MTC at start-up should be considered.

---

<sup>[1]</sup> 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.**

#### Review Results

The Requirement is addressed. Fail safe design is implemented in the most important reactor feature, namely both moderator temperature and the overall reactivity coefficients are negative, and the reactor is designed so that inherent dynamic behaviour compensates for any rapid increase in reactivity (NRC General Design Criterion 11, DCD3.1).

Also the reactor protection system is designed to fail into a safe state (Crit 23, DCD3.1).

In cases where fail safe design is not practicable, detection of failures is assured, or systems are designed as inherently stable or as passive safety systems. Several such systems are listed in point 4.28 dealing with design principles.

The DCD claims that the ESBWR is designed inherently stable, and in addition power oscillations which can result in exceeding acceptable fuel design limits should be reliably and readily detected and suppressed (Crit 12, DCD3.1, also sections DCD 5.2.5, 7.3.3). As the plant includes novel features which potentially influence core stability, the claims of the DCD should be further assessed in the next phase of safety analyses.

Failure signals are created in case of excessive leak rates. In case of RCS leakages, three diverse and independent systems are provided to detect leakages before they develop into breaks. Small leaks are detected by temperature and pressure changes, increased frequency of sump pump operation and increased airborne radioactivity. Large leaks are detected also by changes in flow rates in process lines and changes in reactor water level (Crit. 30, DCD3.1). Process Radiation Monitoring System provides trip signals to the RPS whenever pre-established limits are exceeded (Crit. 13, DCD3.1)

**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. The RCS of the ESBWR is designed according to ASME III, which includes the consideration of transients and fatigue (usage factor).

In addition, the RCS will be subject to in-service inspection as described in Vol. 2, sec.3.1.2.3, in order to be in compliance with criterion 32 of the USNRC General Design Criteria (10 CFR50, Appendix A). Such inspection is designed to detect deterioration of materials caused by various effects.

A material properties surveillance program is foreseen, which will follow a.o. the shift in the nil-ductility temperature and its consequences for the allowed number of operational transients. Vessel material samples are irradiated to follow and predict the actual ageing process of the vessel material. Detailed information is contained in sec.3.9.

Ageing is addressed in various design matters, but a dedicated Ageing Management / Evaluation Program, which should take care of the life time effects (corrosion, erosion, embrittlement, etc.) of a series of structures systems and components (SSC) and their supports, was not found.

The next step detailed assessment of the ESBWR, should study whether the grids used for in-service inspection are fine enough for timely detection of 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 ASME XI requirements do not always cover such effects (crude inspection mesh).

The next step detailed assessment should also investigate to what extent feedwater nozzle thermal shedding concerns (which arose at other BWRs in natural circulation [\[1\]](#)) have been avoided.

A dedicated Ageing Management / Evaluation Program should be developed, if not already present or under development.

---

<sup>[1]</sup> Deep cracks were found in the Dodewaard feedwater nozzle as a consequence of this phenomenon

**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.**

#### Review Results

The Requirement is addressed. Mechanical, electrical and electronic equipment qualification requirements are addressed in detail, pertinent regulations are quoted and the equipment is stated to be qualified for full range of all normal, incident and accident conditions DCD 3.11, that have been considered in the design. Both seismic loads (DCD 3.9.2.2) and environmental parameters of temperature, humidity, pressure and radiation have been considered. The methods of determination of accident parameters are in line with with the requirements of General Design Criteria (GDC) 1, 2, 4, 14 and 30 of Appendix A to 10 CFR 50, as well as Appendix B to 10 CFR Part 50, as discussed in SRP 3.10 Draft Revision 3 (Reference 3.10-1) and Appendix S to 10 CFR 50.

For new components and systems large scale or full size qualification tests have been performed. Qualification tests of the GDSCS were performed in a full-height, scaled volume test facility at GEH (PSR 2.12.2.). When possible, equipment testing was conducted on prototypes of the equipment to be installed in the plant. If not, a detailed inspection and justification of the capacity of the equipment tested was made. Cylindrical components such as CRD housing are qualified by analysis, and more complicated components such as SRV by combination of tests and analysis. The methodology applied is described in detail in (DCD 3.9.2.2.2)

The functionality of valves can be demonstrated by an analysis or by combination of analysis and test. The qualification of electrical and instrumentation components controlling valve actuation is described in section (DCD 3.10).

Determination of radiation doses for normal and accident conditions is addressed in line with the US approach as required by the NRC (DCD 3.11.4.) using NUREG-1465 approach to determine accident doses (DCD Appendix 3H).

The qualification program and methodology are described in detail in the NRC approved licensing Topical Report on GE's environmental qualification program (DCD 3.11)

From the above it is obvious that the classification strictly follows the standard US procedure and thus does not explicitly address the relevant Requirements as formulated in NS-R-1, which are consistent with the formulation of the principles of the UK HSE SAPs. Therefore, there is the need in the next step to review in detail to which extent the classification system used for the ESBWR is implicitly addressing the IAEA Requirements and the SAPs.

**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 has been addressed. The submission addresses the requirement for provisions for the decommissioning the proposed plant. Specific design features that will facilitate the decommissioning programme, especially with regard to reduction of radioactive waste and dose limitation have been highlighted. Provisions for removing, dismantling, decommissioning and disposal of major plant items the plant have been described or postulated.

The selection of materials; design provisions; limitation of radioactive contamination; and identification, storage and retrieval of information have been considered, however, making the facility passively safe before entering care and maintenance phase has not been considered.

The information provided could be enhanced with comment on structural integrity to facilitate the choice of strategies for final dismantling and closure of the plant.

It is suggested that information on long-term integrity of structures to allow deferred strategies for dismantling is requested within any future detailed submissions provided.

## 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 under IAEA Draft Requirement 4.40. The submission addresses the requirement for procedures that cover normal operations and anticipated operational occurrences.

Procedures (18.9) will be provided electronically and will also be available in hard copy meeting the following requirements:

- Presented as logic or flow charts, (where practical);
- Displays will include decision-making aids and requisite steps;
- Checklist of prerequisites or interlocks to steps;
- Allowance of operator access to controls;
- Verification of operator decisions;
- Retention of operator control and authority;
- Logging of decisions;
- Continuous updating of plant parameters and plant status; and
- Written to Human Factors Engineering (HFE) best practices.

The objectives and scope of the procedure development programme are described in the submission (18.9.1). The scope of the procedures addressed includes:

- EOPs including Generic Technical Guidelines (GTGs) for EOPs;
- Plant and system operations (including start-up, power, and shutdown operations);
- Test and maintenance;
- Abnormal and emergency operations; and
- Alarm response.

The procedures aspects in DCD Section 13.5 (Conduct of Operations) and 18.9.2 describe the basis for procedure development including:

- Plant design bases;
- System-based technical requirements and specifications;
- Task analyses results;
- Risk-important HAs identified in the HRA/PRA; and
- GTGs for EOPs.

The section also describes how the procedure programme addresses the requirements specified in 10 CFR 50.34(f)(2)(ii) and describes the Procedure Writers' Guide. It also

references the ESBWR HFE Procedures Development Implementation Plan that describes further details about the following topics:

- Writers Guide
- Procedure Format
- EOPs.
- Procedures verification and validation programme including the use of simulation.
- Computer-based Procedures (CBP) - including an analysis of the available alternatives in the event of loss of CBPs will be also provided.
- Procedure Maintenance and control of updates
- Procedure Access and Use.

Plant Operating (13.5.3.1) and Emergency Procedures (13.5.3.2) Development Plan are described in the submission. Operating and Emergency Procedures (13.5.3.4) include:

- System procedures,
- Off-Normal or Alarm Response
- General Plant Operating Procedures
- Computer-based Procedures (CBP) - including an analysis of the available alternatives in the event of loss of CBPs will be also provided.
- Emergency and other Significant Event Procedures (it is not apparent that this includes severe accident management guidance).

Procedures for Maintenance, Modification Control, Radiation Control , Calibration, and Inspection and Testing will also be provided.

Procedures will also have to take into account the specific requirements (statutory, legal, organizational aspects, etc) of the national Operating organization and Regulatory Body. This would normally be expected to be covered by subsequent submissions. In addition the results of PSA should be used in developing the operating procedures (DS 394 2.31).

**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. Although the staffing requirements will be the ultimate responsibility of the Operating Organization, detail regarding numbers, qualifications and assignments is provided for control and monitoring personnel on the preliminary staffing assumptions (18.6.3) for ESBWR. The assumptions are based on a Staffing and Qualifications Plan (18.6.4) developed through Operating Experience review, Functional Requirements Analysis and Allocation, Task Analysis, Human Reliability Analysis, Human System Interface Design, and Procedure and Training programme Development.

The training programme development (18.10) is addressed in the Chapter on Conduct of Operations (13.2) The submission highlights the possible involvement of the Requesting Party in developing training programmes from providing material for training to the possibility of conducting specific training programmes. Training facilities and resources that may be provided by the Requesting Party include reference training simulator and part-task training simulators. The submission also includes the elements of a Training Programme (18.10.4) that includes training for a full range of positions of operational personnel including licensed and non-licensed personnel whose actions may affect safety. The initial and on-going training programmes are proposed in the submission.

The staffing assumptions are well founded; however, the qualification and experience staffing requirements of the national operating organization will also have to be considered in future 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. The general objectives of the Human Factors Engineering (HFE) Programme (18.1) are stated in human-centred terms, which, as the HFE programme is developed will be refined and used as a basis for HFE planning, testing and evaluation activities. HFE design goals ensure that:

- Personnel tasks will be accomplished within time and performance criteria;
- Human System Interfaces, procedures, staffing/qualifications, training, management, and organizational variables will support a high degree of operating crew situational awareness;
- Allocation of functions will accommodate human capabilities and limitations;
- Operator vigilance will be maintained;
- Acceptable operator workload will be met;
- Operator interfaces will contribute to an error free environment; and
- Error detection and recovery capabilities will be provided

The HFE program addresses the Main Control Room (MCR), Remote Shutdown System (RSS), Technical Support Centre (TSC), Emergency Operations Facility (EOF) displays, and Local Control Stations (LCSs) with a Safety-Related function or as defined by High Level Task Analysis.

The applicable Human System Interfaces, procedures, and training included in the HFE programme include operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures) for those systems that have safety significance.

The Man-Machine Interface System (MMIS) employs digital technology to implement the majority of the monitoring, control, and protection functions for the ESBWR. Standardization of hardware and software, and modularity of design is used to simplify maintenance and provide protection against obsolescence.

Human-System Interfaces (HSI) (18.8.1) are established and evaluated through the HSI Design Implementation Plan that considers:

- Equipment and work place design (illumination, noise, vibration, etc)
- Information and control (displays, controls, alarms, etc)
- Task analysis
- Equipment functions (hardware and software)
- Control Room operations
- Resolution of Human factor engineering (HFE) and HSI issues

Static mock-ups and models, and simulation are utilised to evaluate HFE and HSI issues (e.g access and conduct of operations)

HSI design implementation activities include the development of dynamic models for evaluating the overall plant response as well as individual control systems, including operator actions. These dynamic models are used to:

- Analyze both steady state and transient behaviours;
- Confirm the design of the advanced alarm system concepts;
- Confirm the adequacy of control schemes;
- Confirm the allocation of control to a system or an operator;
- Develop and validate plant operating procedures; and
- Incorporate use of simulators.

Specific design features that will facilitate the decommissioning programme, especially with regard to reduction of radioactive waste and dose limitation have been highlighted (12.6.1). Provisions for removing, dismantling, decommissioning and disposal of major plant items the plant have been described or postulated.

## **4.45–4.48 Defence in depth and margins**

### **4.45–4.48**

**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 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. The ESBWR utilizes the DiD-concept as a basic design philosophy, according to the DCD, sec.6.2.1.1.10.1. As the ESBWR is at one side a well-proven design, which is based on an evolution of a series of BWRs over many years, which complied with the DiD-concept, and at the other side an advanced design which is set up to strengthen the various safety functions, it is expected to meet the DiD concept in full. In addition, GEH has compared the ESBWR with the USNRC safety rules and regulations (see PSR, Table 2.4-1), which include the DiD-concept. GEH has concluded that the ESBWR is in compliance with these rules and regulations.

The fulfilment of the DiD-concept is confirmed by the consideration of various categories of postulated initiating events (PIEs) which each have their acceptance criteria and systems to cope with them. These events range from normal operation, via anticipated operational occurrences and design basis accidents (DiD levels 1 - 3) to beyond design basis events, so-called special events (level 4), and severe accidents (levels 4 and 5). It is noted that the special events - which are still controlled by plant systems - are an important part of the DiD, as they expand plant safety beyond the design basis.

Various improvements have been introduced that strengthen the level 1 DiD. E.g., all recirculation piping has been removed, which effectively reduces the probability for LBLOCA. Core flow depends on natural circulation only (no reactor coolant pumps, RCPs). Containment penetrations have been strengthened to reduce the probability for containment bypass.

In levels 2 and 3 improvements have been achieved by introducing various passive safety systems, e.g. an isolation condenser to remove decay heat.

GEH states that protection against e.g. ATWS has been improved (level 4). In the severe accident domain (levels 4 and 5), GEH states that the probability for Direct Containment Heating (DCH), ex-vessel steam explosions and core-concrete interaction (CCI) have been reduced. An important point is the permanent inertization of the containment, which effectively reduces the risk from hydrogen combustion.

The design has been analysed by the PSA, and various improvements have resulted (sec. 2.6.4.3).

If the statements by GEH are correct, then the conclusion is that the DiD is not only present, but that it has been improved over previous designs. A detailed assessment of GEH's statements is not possible within the limited scope of this study.

On the foregoing basis, the reviewers have the opinion that the ESBWR design has addressed the requirements of the DiD concept.

Various cautions, however, must be expressed and should be subject of the next step safety assessment:

1. As there are no reactor coolant pumps (RCPs), an RCP-trip to mitigate ATWS is not possible. Hence, the remaining mitigative mechanisms in a BWR, such as intentional RPV level decrease, need a careful analysis.
2. Similarly, the absence of RCPs creates a risk for single channel, parallel channel or whole-core thermal-hydraulic instabilities. Although oscillations do not endanger the core a priori, a decreased margin to DNB is possible. In addition, the appearance of oscillations creates an extra, unnecessary burden on the operators. GEH refers to experience gained in early designs, but these are very small compared to the ESBWR, so proper scaling is extremely important. The argument about the value of the fuel time constant should be checked: a larger time constant may introduce a larger phase shift in the void-neutron transfer functions and, hence, decrease stability rather than increase it, as GEH states.
3. No high-pressure injection is available (as in existing BWRs), so the provision of a fast and reliable depressurisation is essential. The absence of high pressure injection system should be extensively investigated.
4. Passive systems have limited driving forces and are, hence, sensitive to line blockage, sticking check valves and failing squib valves, as incidents in the past have shown. Operation of the passive safety systems should be shown to be effective by sufficiently large margins in a detailed assessment, and it should be substantiated that the lessons from past incidents have been learned. The RP claims that limited driving forces have been considered and large margins imposed, and that the reliability of check valves has also been considered.
5. No evidence has been found that the primary coolant lines have been designed for leak-before-break / break preclusion. Such qualification is very beneficial for the level 1 DiD.
6. Proper design of (non-safety) control systems may effectively reduce the number and magnitude of actuations of safety systems and, as such, is an effective mechanism to enhance the level 2 DiD.
7. Important aspects of the level 2 DiD are provisions against disturbance related to the external grid. The plant has a robust connection to the external grid through two independent connections. But it could not be established whether the ESBWR has a possibility for 100% load rejection and the possibility to run only house load ('island operation').
8. Systems that are beneficial for the mitigation of BDBAs have not been classified to any dedicated standard. Such classification is useful to provide assurance that the intended functions indeed can be fulfilled. (This could be inferred from the classification Requirements of IAEA NS-R-1). There is, however, no need to formally classify them as safety systems. Regulatory control over some non-safety systems is, however, considered (Design Control Document, DCD, Ch. 19).
9. A deluge line is present to flood the drywell lower part if a high temperature is sensed, i.e. after RPV failure. No actions seem to be directed to flood the lower part of the vessel and, hence, prevent vessel failure by external cooling. Proper application of DiD requires prevention before mitigation, i.e. flooding could be initiated earlier. Such early flooding could be part of the severe accident management guidance (SAMG) - see later in this list.
10. A core catcher is present (BiMAC), but no documentation was available to assess its effectiveness. The present understanding is that only relatively thin layers of corium can be effectively cooled by core catchers, for which the drywell floor may not offer sufficient space. Although core-concrete interaction (CCI) certainly will be delayed by

the BiMAC, a total inhibition of it may not be possible. Consequently, non-condensables will be generated and containment pressure will rise, eventually until containment failure. A filtered vent (as in many European designs) is not present, but operators can vent the containment from elevated pressures (DCD, ch. 19). Note that a long-duration containment pressure above ambient may also result in substantial releases to the outside via the normal leakage pathways. To accept this occurrence may not be in line with the ALARA-principle.

11. In addition, a severe accident cannot be considered under control as long as not all debris is covered and cooled, which requires flooding of the containment to a level above top-of-active-fuel (TAF) and, for many designs, also containment venting. No dedicated provision has been found to enable this process (for existing BWRs an RPV-vent possibility) but containment venting is possible.
12. Severe accidents can endanger the staff in the control room. No provisions have been found to protect the control room staff against elevated radiation (habitability requirements) of such magnitude. The DCD only specifies DBAs for such evaluation (sec. 6.4). There is an emergency control room (ECR) / emergency shutdown room, which can be used in case the main control room is not habitable any longer. Such an ECR may also offer protection in area events. The habitability of the ECR is similar as the MCR, i.e. it may not be fully accessible under severe accidents.
13. 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. The DCD refers in several places to such SAMG (e.g., Chapter 6, sec. 6.2.5) but does not contain a description or reference to the SAMG. Note that in SAMG, it may be needed to flood the drywell (DW) from the wet well (WW), for which a vent line from the DW to the WW may be needed (see SAMG of existing BWR6 Mark III in Europe and Taiwan). Also possibilities to vent the RPV should be present, as the water level in the vessel ultimately should be above TAF, which may not be achievable without venting the RPV (as addressed already under # 11).
14. A Technical Support Centre, from which the SAMG will be executed, has been provided (Chapter 13, sec. 13.3). It has the same habitability protection as the control room and, hence, may not offer sufficient protection in the case of a severe accident.
15. The risk from hydrogen combustion has effectively been reduced by permanent inertisation of the containment. A remaining risk, although on the long term (DCD, ch. 19) is from radiolysis, which produces both oxygen and hydrogen.
16. SAMDA (severe accident management design alternatives) analysis has not been studied by the reviewers. Note that the consideration of design changes for severe accident management is required under art. 5.32 of the IAEA Requirements on Design, item (3), to the extent which is reasonably practicable.

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 ESBWR-design, but it was not possible within the limited time available to see whether the issues are covered to full depth; and
- sec. 4.48: safety margins are addressed in the ESBWR- 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. A specific and important mitigative safety feature in level 4 of the DiD is the permanent inertisation of the containment.

The ESBWR-concept bases largely on passive safety systems. Although this gives clear advantages, there is also a risk that the driving forces are too small to overcome blockages and sticking check valves. Also the reliability of squib valves should be further investigated, also in the light of incidents from the past.

The DiD-concept in the ESBWR should be carefully analysed, notably where important deviations occur from established practices, as discussed above. Also 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.

The SAMDA analysis needs adaptation to NS-R1, sec. 5.32, item (3). 'Reasonably practicable' should be based on European standards, where available. Examples of items to be studied are the introduction of HPSI and the containment vent.

An important matter is the design and implementation of full package of the SAMG, including the equipment and instrumentation which is needed for its execution.

#### **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. The information on the safety analyses performed for 7 categories of operational modes of the reactor is provided in Chapter 15 of the DCD. In addition a complete release of the radioactive inventory in all tanks containing radionuclides in the liquid radwaste system has been analysed as a bounding unspecified event.

Regarding the post-operational state, the Head Document provides a short summary of design features aimed at minimizing radioactive waste and facilitating dismantling.

Compliance with US NRC Regulatory Guides, Industrial Codes and Standards, Action Plan Items, Generic Issues and US URD requirements is systematically addressed in DCD Chapter 1.9. The ESBWR design is undergoing the design certification process of the US NRC. The report indicates that Final Design Approval is expected in late 2008 and Design Certification in late 2009. The report also makes reference to the experience in licensing the BWRs and ABWRs in foreign countries.

The Head Document makes reference to the safety objectives established by the US NRC and the UK HSE. It is stated that detailed information on compliance with the WENRA reference levels will be provided at the next stage.

**4.50 The safety analysis shall address both the consequences arising from all normal operational conditions (including startup 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 annual collective occupational dose is estimated in DCD Chapter 12.4. It is described in the Head Document that based on experience the methodology used is very conservative. Therefore, the best-estimate prediction for the ESBWR is 220 man-mSv/reactor-year. Table 2.2-1 of the Head Document provides a summary of the radiation exposure estimates for workers and the public for normal operation and DBAs.

Results of the accident analyses are presented in DCD Chapter 15. However, the analyses follow the standard US NRC procedure. Also, for calculating radiological consequences the standard NRC procedure is followed. In order to address these differences from the categories of the IAEA Standards and the more detailed SAPs, the Head Document Table 2.2-1 provides information on how the US categories relate to the categories of fault sequences contained in the SAPs of the UK HSE.

Initial start-up testing programmes are described in DCD Chapter 14. No information is included regarding special tests for a first-of-a-kind plant to verify parameters for the performance of innovative safety features, in particular passive systems. However, test results from experiments are summarized in 1.5.3.

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. However, very limited information is included related to the BiMAC, which has been developed to the conceptual design level only.

Regarding severe accidents it is claimed that a “full-scope (Level 1, 2, 3) PRA, that covers both internal and external events, for at-power and shutdown conditions” has been prepared. The PSA is not included in the documentation and the reference given could not be reviewed. DCD Chapter 19 and Chapter 6 of the Head Document provide a short summary of the PSA Level 1 results. Depending on the complexity and uncertainty in processes bounding assumptions are used. Regarding Level 2 aspects it is reported that the ‘Risk Oriented Accident Analysis Methodology’ (ROAAM) has been developed as a bounding, rather than best estimate, method. DCD Subchapter 19.6 concludes that the US NRC requirements and safety goals are met.

Though more detailed, the SAPs probability categories are consistent with the categories of IAEA Requirements. It is suggested that for the next stage of the review additional information consistent with the IAEA or the SAP categories be provided.

It is noted that in spite of bounding assumptions the PSA is resulting in very low frequencies for severe accidents. The PSA will need to be reviewed in detail at the next step.

The next step of the review should include information on the test procedures for the first-of-a-kind innovative design features.

More information needs to be provided on the performance of the BiMAC.

**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<sup>1</sup> 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<sup>2</sup>. 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. As described in Document 1 Chapter A.3.3 and DCD Chapter 15 the selection and grouping of anticipated operational occurrences and accident conditions within the design basis follows the standard US NRC procedure. Internal and external events are included. In line with the rules of a deterministic safety analysis partial or complete failure of components is assumed. Conservative bounding assumptions are made.

Chapter 2.12 of the Head document provides a summary of the functioning of the innovative features. A description of the related test programmes including major ESBWR unique test programmes and scaling of tests is described in DCD Chapter 1.5.3. In particular reference is made to a comprehensive list of related GE reports. Considering the small size of the Dodewaard reactor, the scaling of natural circulation behaviour deserves particular attention.

Main Steam Line Breaks inside and outside of the containment are analysed as bounding Design Basis Events based on conservative assumptions in accordance with US NRC procedures and include an assessment of radiological consequences.

A brief summary of the PSA is provided in DCD Chapter. A summary of numerical results is provided in Chapter 6 of the Head Document. The test programmes related to the innovative passive features of the ESBWR including major ESBWR unique test programmes and scaling of tests will need to be reviewed at the next stage.

The PSA will need to be reviewed at the next stage with particular attention to the very low frequencies for severe accidents (e.g.  $1.2 \text{ E-8/year}$  for CDF from internal events at power). It is noted in the documentation that contributions to CDF translate to very low frequencies and that the model converges at  $1\text{E-15}$ .

The categories of LOCA sequences described in DCD Chapter 19 are different from the categories used in the Head Document providing the numerical estimates.

---

<sup>1</sup> 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).

<sup>2</sup> 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 ESBWR Design Control Document (DCD) describes the main elements of both the deterministic safety analysis and probabilistic risk analysis, in PSR secs. 2.5 and 2.6.

It can be concluded that the ESBWR follows the USNRC's quality group classification (Reg. Guide 1.26), regarding the deterministic design analysis. Criteria of other Standards re-classification, such as the ANSI/ANS 58.14 and the draft IAEA Guide NS-G.1.14 go beyond the recommendations of RG 1.26. An assessment of whether these higher-level and more elaborate criteria also are met and this should be part of the next step safety assessment.

The PSA was also used to implement several design enhancements (DCD, sec. 2.6.4.3). Further evidence that the safety analysis incorporates deterministic and probabilistic approaches is provided in sec.15 'Safety Analyses', sec.19, 'Probabilistic Risk Assessment and Severe Accidents' and sec.17, 'Quality Assurance' and sub-section 17.4, Reliability Assurance Program During Design Phase. Examples in Sec.19.2.2.1.1 include enhancement of the design, enhancement of safety, reduction of overall risk profile, satisfying or exceeding the safety intent of risk goals, and assessing technical specifications surveillance intervals and allowed outage times by the use of PSA.

As such, it can be concluded that an integrated decision making process was followed. The next step safety assessment should confirm this approach on the basis of more detailed documentation, including the PSA.

**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. Vol. 2, Chapter 3, describes compliance with USNRC criteria, which includes compliance with RG 1.26, quality group classification. Non-safety systems - which play a role in mitigating non-core melt BDBA and severe accidents - are subject to regulatory oversight, according to Vol. 2, Chapter 17. Vol. 1, Chapter 5 describes how the deterministic analysis has been carried out. The analysis has been done for all events within the design basis, plus a number of 'special events', outside the design basis, but for which protection is offered. Examples of these events are ATWS and station black-out.

Systems are available to mitigate the consequences of these and other BDBA, not being core melt accidents, and core melt accidents. For the non-core melt accidents, Vol.2, Sec. 17.4 specifies certain requirements, in conjunction with the D-RAP (Design Reliability Assurance Program). These are limited to operation, maintenance and monitoring (Vol. 2, Ch. 17, Sec. 17.4.4). No specific safety class and associated design requirements for the equipment involved in the mitigation of these events was found.

In addition, criteria of other Standards re classification, such as the ANSI/ANS 58.14 and the draft IAEA Guide NS-G.1.14 go beyond the recommendations of RG 1.26. An assessment of whether these higher-level and more elaborate criteria also are met was not made, although some use of the ANSI/ANS-standard was mentioned (Vol.2, Sec. 3.2.2).

An overview statement of the approach, scope, criteria and output of the deterministic safety analyses is presented in section 2.5 of the preliminary safety report. The key to the approach to plant safety is a nuclear safety operational analysis (NSOA). The safety analysis is consequences oriented, focusing on the limiting response to the event, while the NSOA is system oriented, focusing on the system level required actions necessary to bring the plant to a stable configuration.

It is stated that for anticipated operational occurrences, the reactor core and associated coolant control and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of AOO (15.03.1).

It is mentioned as well that the radiological analysis is based on conservative assumptions considered to be acceptable to the NRC for the purpose of determining adequacy of the plant design to meet 10CFR 50.34 guidelines (15.4.1.4, 15.4.5.5, ...).

Although conservative assumptions are frequently mentioned, mainly for radiological analysis, the use of a deterministic approach is never mentioned in Chapter 15. Tables of

acceptance criteria, both with respect to design rules and radiological consequences, are specified in the Preliminary Safety Report, e.g. Table 2.5, which give confidence of conservative design.

The preliminary conclusion is that for DBA and selected BDBA, conservative deterministic rules and requirements have been followed. However, this statement should be verified in depth. For BDBAs in general and severe accidents in particular, this could not be established from the documents studied. A process is in place to formally control operating requirements of the associated equipment.

1. Classification to more recent industry and international standards (ANSI/ANS 58.14 and IAEA NS-G 1.14) should be executed to enhance the safety classification and the associated design requirements.

2. In the area of non-core melt BDBAs and severe accidents it should be investigated how classification is structured and what design requirements and rules are defined for the relevant equipment, beyond what is specified in sec. 2.5 of the preliminary safety analysis report (e.g. Table 2.5). The selected design rules and the margins obtained should be further studied, 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 partially addressed. (This Requirement is complemented by further Requirements of NS-R-1, in particular Requirement 5.37).

The PSA is very briefly described in DCD, Chapter 19C (Probabilistic Risk Assessment and Severe Accidents). References are repeatedly made to the PSA report NEDO-33201, (Reference 19.1-1) which is docketed as part of the ESBWR DCD application, but was not available for the review. However, the PSA results and important methodological details and assumptions are not provided in DCD, Chapter 19. Overall results and general aspects are presented in Chapter 2.6 of the general part of the preliminary safety report (PSR). There are also some relevant inconsistencies between these two parts of the documentation.

The PSA includes Level 1 PSA for internal initiating events, and with several limitations Level 2 and 3 PSA, the analysis of hazards and non full power operation modes. Thus, the level 3 PSA is not described (it is only explained that the safety goal is met with a very large margin), and fires and floods are analyzed without knowledge of cable and piping routing. It is claimed that fires make no substantial contribution to risk. However, the PSR shows that internal initiating events and fires make the same contribution to risk.

The PSA is largely based on bounding approximations and generic data and is poorly documented in the DCD. Very limited information on methods applied and result insights is provided. In many aspects, the summary information about the PSA in the PSR is more relevant than the one provided in the PSA report (Chapter 19), and there are also contradictions between both parts, e.g. on the initiating event definition and grouping. Relevant risk contributors in the level 1 according to the PSR, e.g. fires, are neglected and not considered for the level 2 and 3 PSA.

A solid documentation of the analysis, methods and assumptions used is not provided. The very low risk results obtained with even with bounding or very conservative analyses or assumptions require a detailed review to be performed at the next step.

The IE identification process is not described and leads to different types of LOCAs, depending on size and location and transient categories. The acceptance criteria for main safety functions is given in Chapter 19, e.g. maximum peak cladding temperature for core cooling function, but success criteria for safety systems are not given. There is no indication of the kind of accident analysis calculations performed for developing success criteria, accident sequences and associated available times for human interventions. There is no indication on sequence end states and type of grouping for interface with the level 2 PSA.

The PSA is based on generic industry data for component failures and initiating events. No further details are provided in this regard in Chapter 19. It seems that no uncertainties of the input data are considered, since the principal source does not provide them.

System analysis, the largest part of the level 1 PSA, is not documented. It is only indicated that credit is taken from safety and no safety systems and the type of failures included in the models.

In DCD Chapter 19, the results of the internal event analysis just point at common cause failures as typical dominant risk contributors and at two manual actions. A so called distillation of the PSA presents the results in terms of the functional failures and successes of the 10 dominant accident sequences. Table 19.2-3 does not summarize the important initiating events, operator actions, common cause failures (CCF), SSCs, assumptions, and insights from importance, sensitivity, and uncertainty analyses, as indicated in several parts of CDC Chapter 19. Subsection 19.2.5, "Summary of overall plant risk results and insights" does not provide them. A CDF of  $1.22 \text{ E-}08/\text{y}$  is reported in the PSR, Figure 2.6.1. of this report provides the relative contributions of the IEs. However, these IEs do not match with those indicated in Chapter 19. These reflect deficiencies in the QA processes.

It is stated in Chapter 19 that the ESBWR has a low potential for generating large releases and that the sequences that would have this result are unlikely and involve large uncertainties. Therefore, a bounding, rather than best estimate, method is used for assessing containment performance. The Risk Oriented Accident Analysis Methodology (ROAAM) methodology is used and 3 important severe accident phenomena, ex-vessel steam explosions, ex-vessel debris cooling, and long term containment over pressurization, are analysed.

PSA level 3 is not described. It only explained that the safety goal is met with a very large margin. The PSR (2.6.6.2 and table 2.6-3) gives a "probability" of receiving a dose greater than 0.25 Sv at 0.5 miles of  $2\text{E-}09/\text{reactor-year}$ . Other parts of the documentation also express "probabilities" with dimensions of  $[\text{t}^{-1}]$ .

Internal fires (named as external event fire) have been analysed without specific knowledge of cable routings, ignition sources, and target locations in each zone of the plant. In spite of using a simplified conservative bounding analysis, with no credit for fire suppression and distances between fire sources and targets, and even consideration of failures of fire barriers, a CDF estimate of  $1.22 \text{ E-}08/\text{reactor-year}$  is given in the PSR. These very low results represent 99% of the CDF of internal events, but it is concluded that there are no dominant risk contributors and impact of fires on LRF and outside consequences is not calculated, as the analysis for CDF is considered bounding. The analysis of internal floods without knowledge of piping layout uses a bounding approach and is of a similar nature. The PSR shows a CDF due to floods of 30% of the CDF due to internal events. The results are not propagated to the

level 2 and 3 PSA. High winds are considered not important. A qualitative justification for the plant to be able to cope with the effect of tornados is provided.

Four important IEs for low power and shutdown are identified. One operator action is considered significant. There are no significant random failures. According to the PSR, the risk during shutdown from only internal events adds 72% of the risk of power operation from internal events. In addition fires during shutdown are the single largest contributor to the total CDF and contributing nearly twice the CDF due to internal events at power operation (PSR Table 2.6-2). Since relevant shutdown modes consider the containment open, it is assumed that CDF progresses to LRF. However, it is not very clear why in such case offsite consequences are considered negligible and therefore results of the level 1 are not passed to the level 2 and 3.

## 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 national regulatory body addressing the applicable fundamental safety objective and fundamental safety principles established by IAEA SF-1. (No operator has yet been determined.)

Criteria defined by the designer: The ESBWR is an evolutionary design. It is stated that as much as possible the ESBWR builds on the design features of operating BWRs. The Head Document and the DCD Chapter 1 make extensive reference to the development of the ESBWR as a long-term evolutionary process making use of the experience gained. Extensive reference is made to the regulatory and utility requirements addressed and to the experience in licensing BWRs and ABWRs in foreign countries.

The basic approach to the safety assessment is deterministic complemented by probabilistic analyses. The analyses and the documentation submitted follow the US NRC procedure and are documented in the standard DCD format. The accident analyses include an assessment of the radiological consequences in accordance with US NRC requirements. As a conservative approach to containment performance major core degradation and melting is assumed though the analyses show that core integrity is maintained.

In DCD Subchapter 19.2 it is claimed that the ESBWR PRA is a “full-scope (Level 1, 2, 3) PRA that covers both internal and external events, for at-power and shutdown conditions”. The PSA itself is not included in the documentation and thus could not be included into the review at this stage. DCD Chapter 19 gives a short summary of PSA Level 1 results. The Level 2 PSA has been developed as a bounding analysis. Potential Large Release Sequences and containment performance are briefly summarized. Consequence calculations from internal events are included in the Head Document in Figure 2.6-2. The results of the PSA demonstrating compliance with the US NRC goals by large margins are given in Table 2.6-3.

The ESBWR design is undergoing the design certification process of the US NRC.

The innovative Basemat Internal Melt Arrest and Coolability Device (BiMAC) (DCD Chapter 19.3.2.6) has been developed to the conceptual design stage only. No criteria for the functioning of the BiMAC are yet available.

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.

Detailed reference is made to the differences in safety objectives and criteria established by the US NRC and the UK HSE. Table 2.2-1 provides a comparison of US and UK radiation exposure goals for normal operation and accident conditions. It is recognised that the SAP NT.1 Numerical Targets and Legal Limits "do not precisely line up against the US basis". It is indicated that a specific UK compatible assessment will be performed at a later date in the review process.

Since the PSA is only briefly summarized and not included in the documentation it should be reviewed in detail at the next step. It is noted that the CDF from internal events at power ( $1.2 \text{ E-8}/\text{reactor-year}$ ), at shutdown states ( $8.8 \text{ E-9}/\text{reactor-year}$ ) and the internal events LRF (in the range of  $1.0 \text{ E-9}/\text{reactor year}$ ) are very low in comparison to other reactors in spite of the fact that conservative bounding assumptions have been made. The Level 2 and 3 PSA results will strongly depend on the performance of the BiMAC, which is in the state of a conceptual design only. Detailed information needs to be provided to be reviewed at the next step.

It is noted that there are differences in concepts between the criteria used by the designer (meeting the US URD requirements and based on US NRC procedures) and by the UK HSE. In particular the differences in criteria relate to the definition of categories for fault sequence analyses, calculation of radiological consequences and the use of PSA.

Additional analyses will be needed at the next step to demonstrate that the expectations set out in the UK HSE SAPs are met.

## **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<sup>1</sup> 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. The conservative Acceptance Criteria for Infrequent Events and Accidents are given [PSR Tab.2.5-4 and 2.5-5].

The core layout includes treatment of a number of uncertainties [DCD Ch.4.4.2-4.4.3]. For the assessment of the fuel behaviour worst-tolerance assumptions or statistical distributions are used [DCD Ch.4.2.3.1]. The stability analysis includes uncertainties from the model, experiments including scale-up considerations, the plant, the process measurement errors and manufactory tolerances [DCD Ch.4 4D1.2].

The containment analysis incorporates conservative initial conditions [DCD 6 Tab.6.2-6].

The PRA Methodology includes uncertainty assessments [DCD Ch. 19.2.3.1.2]. Uncertainties evaluated from experience and judgments and deviations between predicted and (scaled) experimental results are used in the Probabilistic Analysis for containment pressure fragility [DCD Ch. 19 C 1.5].

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

---

<sup>1</sup> 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.

and BDBA sequences. This might call for sensitivity analyses and scaling effects studies, which have to be assessed carefully. Sensitivity studies with safety codes are not reported and should be presented for detailed review at the next step.

The adverse interactions between active and passive systems are systematically evaluated [DCD Ch.19 A.6.1].

Pilot or demonstration plants are not considered because of former nuclear power plants with natural circulation although the power level was much lower than for the ESBWR.

## 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

Most components of the ESBWR are based on proven designs. However, several novel features have been implemented [PSR Ch.2.12].

Core cooling occurs only through natural circulation. The TRACG code – a modified version (for BWR) of the worldwide accepted TRAC-code is used for estimating core cooling and stability analysis; some experimental and operational data are used for validation purposes [ DCD Ch. 4D, DCD Ch.4.4].

Several thermal-hydraulic and neutron data will be tested in an Initial Test Program [DCD Ch.14].

The loads on fuel rods and fuel assemblies during operation and different burnups are evaluated mainly with the GSTRM code using worst tolerance assumptions [DCD Ch.4.2.3.1]. No comparisons are presented between GSTRM calculations and operational or experimental data at high burnups.

The TRACG code is used to calculate the thermal-hydraulic containment behavior sequences up to accidents, including the Passive Containment Cooling Systems and the Suppression Pool behavior [DCD Ch. 6.2.1.1.3]. Additional information about TRACG can be found in DCD 15.2. However, no experiments (although existing) are presented for code validation purposes.

For PSA CAFTA is used as the fault tree model, MAAP for success criteria and MACCS2 for the consequences [PSR Ch. 2.6.57].

The containment pressure capability was deterministically calculated [DCD Ch.19B] in addition to the probabilistic analysis for the containment pressure fragility [DCD Ch.19C]. No codes or its validation are presented.

No computer codes or calculations for simulating the component and system behavior are presented.

The documentation for the next step review should include:

- a detailed list with computer codes used for safety purposes and its validation.
- more details (tests, computer codes, scaling considerations) about the in-vessel core retention device

## 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 addresses both operating experience utilised in the design and also the need for a continuing programme for the life of the plant through the Owner Reliability Assurance Programme.

Utilization of Reactor Operating and Testing Experience in the Development of Test Programme is described in 14.2.4, which highlights that the operational experience and knowledge gained from previous BWR plants and other reactor types has been factored into the design and test specifications of ESBWR systems and equipments that are demonstrated during the preoperational and start-up test programmes. Additionally, reactor operating and testing experience of similar nuclear power plants obtained from NRC Licensee Event Reports, Institute of Nuclear Operations (INPO) correspondence, and through other industry sources are utilized to the extent practicable in developing and carrying out the initial test programme.

An example of current and topical operating experience being utilised is described in 15.3.7 Control Rod Withdrawal Error during Refuelling.

The submission highlights that Operational reliability assurance activities (17.4.10) are implemented by the ESBWR owner/operator, and uses the information provided by the Requesting Party.

The operating experience review (OER) (18.3) supports HFE by identifying HFE-related safety issues. OER topics include experience from:

- Predecessor plant(s) and systems;
- Experience in industries with applicable systems;
- Industry HSI experience;
- Risk-important HAs;
- Specifically-identified industry issues; and
- Issues identified by plant personnel.

The results of the OER are summarized in the OER Results Summary Report (RSR). The RSR provides the OER process description along with the analyses that were used. These include:

- List of risk important HAs from the predecessor plant and their resolutions;
- List of risk important HAs from the OER requiring special attention in the design process;
- Personnel interviews conducted at predecessor plants with summarized results;
- Sources of OER information; and
- Summaries of OER issues and improvements.

Operating experience will be fed back according to the TMI-action plan (NUREG 0737). The focus here is, however, on operating procedures.

Neither data collection as addressed in the Requirement nor a reference to safety performance indicators was found in the documents submitted, so this matter should be subject of the next step detailed assessment. It should be noted, however, that some collection of data is envisaged as the design includes consideration of anticipated transients (art. 4.35).

In addition, the Requesting Party's Owners Group has extensive experience with the system of safety performance indicators, as this is widely used in US based BWRs. It is anticipated that this experience also will be available to the present application.

Detailed information contained within the submission also includes information on design changes "GENE QA Program Description", NEDO-11209-04A (Reference 17.1-1) Section 16, establishes the Corrective Action programme used during design of ESBWR (17.1.16 Corrective Action).

Operational reliability assurance activities (17.4.10) are implemented by the ESBWR owner/operator, and use the information provided by the Requesting Party GE. Elements include:

- Problem Prioritization: Identification for each of the risk-significant SSCs of the importance of that item as a contributor to its system unavailability and assignment of priorities to problems that are detected with such equipment.
- Corrective Action Implementation: Carrying out identified corrective action on risk significant equipment to restore equipment to its intended function in such a way that plant safety is not compromised during work.

- **Plant Aging:** Some of the risk-significant equipment is expected to undergo age related Degradation and require equipment replacement or refurbishment.
- **Programmatic Interfaces:** Reliability assurance interfaces related to the work of the several organizations and personnel groups working on risk-significant SSCs.
- **Maintenance Rule Program:** A procedure is to be developed by a licensee to implement a Maintenance Rule programme

## 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 at this stage. The Head Document ‘ESBWR – UK Preliminary Safety Report’ is specifically aimed at addressing the requirements of the UK HSE Step 2 request. As a reference for more detailed information it is complemented by the ‘ESBWR Design Control Document’ which uses as a guide the format and content recommendations of Regulatory Guide 1.70, Revision 3, ‘Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants - LWR Edition,’ November 1978.

The information provided in the DCD strictly follows US NRC standard procedures. The level of detail of the DCD goes beyond the present UK HSE Step 2 request. Due to the well-known standard format it provided easy reference to support statements made in the Head Document. The safety analyses are presented in Chapter 15, including the initial conditions (Table 15.5-2), Equipment Performance Characteristics (Table 15.5-3), Event Classifications and Radiological Acceptance Criteria (15.0-7), and other parameters used in safety analyses. For each accident the possible causes are identified, the sequence of events, systems operation, core and system performance, barrier performance and finally radiological consequences are described (Chapter 15, all sections).

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. It is recognised in the Head Document that in some cases the expectations set out in the UK HSE SAPs “do not precisely line up against the US basis”. It is indicated that further analyses will be performed.

The review also showed several areas where the US approach does not explicitly address Requirements of the IAEA Safety Standards or the UK HSE SAPs. These include e.g. categorization of events/accidents, classification safety functions/systems, accident consequence calculations, use of SAMDA assessments, and issues related to PSA. These areas 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 stability of the natural circulation, removal of high pressure injection, functioning of passive safety systems, assessment of scaling effects, increased burn-up, extended plant life, mitigation of severe accidents including the functioning of the BiMAC, PSA related issues, uncertainty analyses

related to core layout, stability analysis, 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

Design of components, structures and systems is presented in Vol. 3, with all possible modes of failure addressed. For seismic loads and external hazards in-depth strength analyses are presented. (Vol. 3, App. A-G). Structural analysis and design, failures modes, design loads, load combinations, and stability requirements are presented for the reactor building and for all buildings containing safety related systems.

The robustness and reliability of individual components is addressed in Chapter 3H on equipment qualification design environmental conditions.

The modelling assumptions used in accident analyses are presented. The thermal hydraulic codes validation is described thus reducing the need to go into detailed presentation of methodology of these calculations. On the other hand, for radiological calculations the reference is made to Alternate Source Term (AST) dose methodology as given in Regulatory Guide 1.183, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors" In addition specific formulae used, for e.g. aerosol removal process description, are discussed.

An example of robustness of safety assessment is provided by the analysis of 15.4.4 Loss-of-Coolant Accident Inside Containment Radiological Analysis. This event assumes a worst case of piping break inside containment so as to demonstrate to what level the acceptance criteria are met for ECCS and the containment. The postulated event represents the envelope evaluation for liquid or steam line failures inside containment.

It is claimed that there are no realistic, identifiable events that would result in a pipe break inside the containment of the magnitude required to cause a LOCA coincident with a Safe Shutdown Earthquake (SSE). The subject piping is of high quality, designed to nuclear construction industry codes and standards, and for seismic and environmental conditions. However, because such an accident provides an upper limit estimate for the resultant effects for this category of pipe breaks, it is evaluated without the causes being identified (15.4.4.1).

**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.

a) There is no specific discussion of the events chosen for analysis, but it is indicated that operational experience with similar plants has been taken into account. The contents of the SAR follow RG 1.70. A list of ESBWR events associated with operating modes is shown in (Table 15.1-3), the rules for event analysis are defined in Table 15.1-4, and the event and instrumentation matrices are presented in Tables 15.1.5-7.

b) The modelling of AOOs and accidents, and the assumptions made in safety analyses are shown and discussed in Chapter 15. Computer codes used in the analyses are described in various chapters, e.g. those for seismic analysis in Chapter 3C and for each of them the description, information about code validation and the extent of its application are provided.

c) The criteria for the determination of safety analysis acceptance are presented in section 15.0.3 for Anticipated Operational Occurrences, Infrequent Events, Accidents and Special Events.

d) The first section of Chapter 15 presents Nuclear Safety Operational Analysis, the second Analysis of Anticipated Operational Occurrences, in the third various types of accidents are considered as usual in the US practice and the fourth section presents analyses of special events with station blackout, ATWS and other level IV accidents.

e) Based on the analyses it is claimed that the consequences of accidents are well below values recognized as acceptable by the US NRC. For example the analysis of the worst case pipe break inside the containment, shown to involve unrealistically conservative assumptions, is based on NUREG-1465 alternative source terms (AST) and the methodology in Regulatory Guide (RG) 1.183, and demonstrates compliance with the 10 CFR 50.34(a)(1), SRP 15.0.1 and RG 1.183 total effective dose equivalent (TEDE) acceptance criteria.

General conclusions on the acceptability of the ESBWR design are made separately for each case of accident considered and the hazards are shown to be much below the acceptable values. The discussion of additional measures possible is made in connection with the probabilistic risk assessment and severe accidents as presented in Chapter 19. PRA results and insights are presented in section 19.2 and the conclusions from severe accident analyses in section 19.3.

Necessary improvements and additional measures are discussed in section 19.A.8, which considers regulatory treatment of non safety system RTNSS. Regulatory oversight level is proposed for each RTNSS and its safety significance is determined to ensure that it has sufficient reliability and availability to perform its RTNSS function, as defined by the focused PRA, or deterministic criteria. For those systems that do not have high risk significance like Alternate Rod Insertion or Standby Liquid Control System Actuation for ATWS, the proposed level of regulatory oversight is at the level of Availability Control Manual, while for the high risk systems like the portions of Diverse Protection System that provide capability to manually actuate ECCS and containment isolations, is contained in Technical Specifications.

The Basemat-Internal Melt Arrest and Coolability System (BiMAC) function has been developed to a conceptual level, with several design details that are not yet finalized. These details are needed to justify the target failure probability of  $1.0 \text{ E-}3$ . BiMAC plays an important role in mitigating core melt scenarios. Therefore, it is a candidate for RTNSS consideration. (19A.8.4.6).