

International Atomic Energy Agency

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

Nuclear Installation Safety Division

REVIEW SUMMARY REPORT

3 March 2008

REPORT CONTENTS

INTRODUCTION

1. BACKGROUND
2. OBJECTIVES AND SCOPE OF THE IAEA REVIEW
3. PROJECT ORGANIZATION AND CONDUCT
4. SUMMARY OF REVIEW RESULTS
 - 4.1 ACR-1000
 - 4.2 AP1000
 - 4.3 EPR
 - 4.4 ESBWR

REFERENCES

ACRONYMS

ATTACHMENT 1 – REVIEW SHEETS FOR ACR-1000

ATTACHMENT 2– REVIEW SHEETS FOR AP1000

ATTACHMENT 3– REVIEW SHEETS FOR EPR

ATTACHMENT 4– REVIEW SHEETS FOR ESBWR

EDITORIAL NOTE

- This report documents the work conducted and the principal results obtained by an international panel of senior experts. The observations and recommendations provided are for further consideration by the UK Health and Safety Executive (HSE).
- The present evaluation was conducted against a selected set of IAEA Safety Standards and was not based on the criteria and structure for the UK Generic Design Assessment, Part I – HSE NII Requirements.
- External experts engaged in the IAEA New Reactor Design Evaluation Project were recruited with the utmost care to ensure neutrality of purpose and commitment to technical excellence of the review.
- The mention of names of specific companies or products does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

REVIEW OF PROPOSED NEW REACTOR DESIGNS FOR HSE

INTRODUCTION

As a response to renewed interest in the development of nuclear energy capacity across the globe, vendors are designing new reactors to meet the growing demand for safer and more economical nuclear power generation. Governmental regulatory bodies will be conducting detailed evaluations of these designs to support licensing decisions. The IAEA Division of Nuclear Installation Safety (NSNI) has developed a tailored project framework to provide Member States with an early evaluation of a vendor's submission of a new nuclear power plant design, including the technical documents pertaining to the reactor design and supporting evidence of its safety features (safety case), against the IAEA Safety Standards at the fundamentals and requirements level. This review framework builds upon design review services which have been conducted by the IAEA over the last 20 years. In offering this support to its Member States, the IAEA fulfils the fundamental goal of promoting global nuclear safety by fostering the application of its Safety Standards.

It should be noted that the IAEA Safety Standards, at the fundamental and requirements level, are generic and apply to all nuclear installations. Therefore, it is neither intended nor possible for the evaluation process to be sufficiently detailed to cover licensing activity, or to constitute any kind of design certification. Moreover, the review does not evaluate the implementation of the requirements, nor does it address the correctness of technical claims made by vendors.

The objective of the review is essentially to examine the comprehensiveness and the completeness of the vendor's safety case in relation to the IAEA Safety Standards. The aim of this new project framework is to provide an early harmonized appraisal of safety cases made by vendors as a basis for an individual evaluation or the licensing process, which remains a sovereign activity of the Member States. Consequently, such safety evaluations, conducted against selected sets of Safety Standards, contribute to more effective management of subsequent activities within a global framework consistent with a harmonized approach to safety worldwide. The work of WENRA highlights the usefulness of the IAEA Safety Standards as a well established basis for the development of reference levels for nuclear safety in Europe.

1. BACKGROUND

The UK Health and Safety Executive (HSE) are considering four new reactor designs under their arrangements for Generic Design Assessment [1]. These designs have been submitted by AECL, AREVA, GE-Hitachi and Toshiba-Westinghouse, known as the Requesting Parties. As part of their design safety assessment HSE wish to take account of international knowledge and information relevant to assessing these designs. Therefore, HSE requested the IAEA Nuclear Installation Safety Division of the International Atomic Energy Agency to carry out an evaluation against the IAEA Safety Standards of proposed new reactor designs which are subject to a Generic Design Assessment (GDA) in the UK. According to the terms of reference agreed by HSE and the IAEA for this assessment, work undertaken by the IAEA was based on design documentation which was publicly available on the 17th of September 2007.

2. OBJECTIVES AND SCOPE OF THE IAEA REVIEW

The objective of the work performed at the request of HSE was the evaluation of the four reactor designs by an international team of senior experts against selected and applicable IAEA Safety Standards to identify completeness and comprehensiveness of the safety cases submitted by the Requesting Parties as required for Step 2 of the HSE Generic Design Assessment. As the principal basis for evaluation, the IAEA Draft Safety Assessment Requirements were selected. These Safety Assessment Requirements are high level standards addressing broadly and generically the safety issues for nuclear installations and activities. The IAEA Safety Standards are developed with the assistance of the Commission on Safety Standards, comprising senior officials of IAEA Member States' regulatory authorities and four thematic committees. They reflect in a consensual manner national regulatory rules and guidelines and embody current best practices. Industrial standards and codes complement the IAEA Safety Standards.

Developed as a logical and hierarchical framework of objectives and principles for fostering nuclear reactor safety, the standards are composed of three categories:

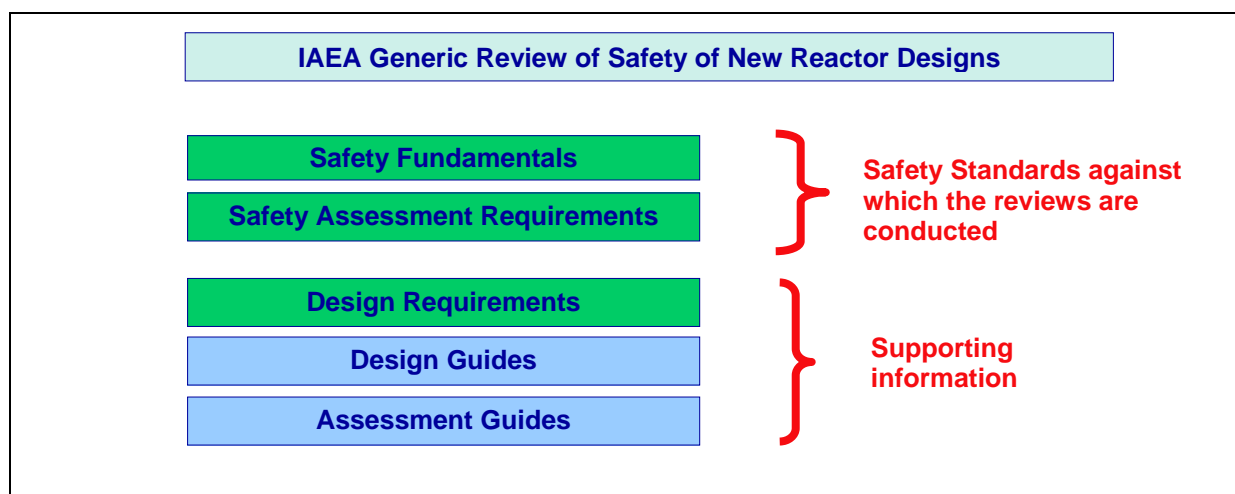
- Safety Fundamentals, which state the basic objectives, concepts and principles involved in ensuring protection;
- Safety Requirements, which specify requirements that must be satisfied in order to ensure safety for particular activities or application areas, these requirements being governed by the basic objectives, concepts and principles stated in the Safety Fundamentals;
- Safety Guides, which supplement the Safety Requirements by presenting recommendations, based on international experience, regarding measures to ensure the observance of safety requirements.

Safety assessment activities are one of the key IAEA Fundamental Safety Principles [2]. These safety fundamentals provide the overall requirements for safety assessment, specific requirements that relate to the assessment of features relevant to safety, the need to address defence in depth and safety margins, safety analysis, the documentation of the safety assessment and the need to carry out an independent verification.

The IAEA Requirements for safety assessment complement the IAEA Fundamental Safety Principles [2], in particular Principle 3, Paragraphs 3.15, 3.16, 3.17. These Requirements are written in a generic manner and are independent of specific technology. Therefore, as the objective of the new reactor design safety evaluation was to assess the completeness and comprehensiveness of the safety cases presented by four different Requesting Parties, the review of the provided documentation concentrated on the Requirements for safety assessment. The review evaluates whether the Requirements are addressed in the design and supplied documentation and if references to technical supporting information are made. In addition, apparent gaps and weaknesses of the overall safety case are identified. It should be noted that the evaluation does not attempt to compare the different reactor design safety cases and makes no reference to comparative aspects of the four designs.

The evaluation focussed in general on assessing if the presented safety cases had addressed the Requirements specific to the reactor design, without consideration of sites or plant management during operation. However, generic site envelope issues were addressed as well as use of operational experience for the design of safety features of the reactors. A more detailed level of the IAEA Safety Standards, the Safety Guides, was used for clarification and interpretation of Requirements only. In a similar manner, the Requirements for nuclear power plant design [3] were used as supporting applicable Requirements for safety assessment. The application of the IAEA Safety Standards for this project is illustrated in Figure 1 below.

FIGURE 1



The following Safety Requirements were considered as the basis and roadmap for the review.

Safety Assessment for Facilities and Activities (Draft – DS348) [4]

- Overall requirements for safety assessment (4.1 – 4.15)
- Assessment of the potential radiation risks (4.19)
- Assessment of safety functions (4.20 – 4.21)
- Assessment of site characteristics (4.22 – 4.23)
- Assessment of radiological protection provisions (4.24 – 4.26)
- Assessment of the engineering aspects (4.27 – 4.37)
- Assessment of human factors (4.38 - 4.40)
- Defence in depth and safety margins (4.45 – 4.48)
- Scope of safety analysis (4.49 - 4.52)
- Approaches to safety analysis (4.53 – 4.55)
- Criteria for judging safety (4.57)
- Uncertainty and sensitivity analysis (4.58 – 4.59)
- Use of computer codes (4.60)
- Use of data from operating experience (4.61)
- Documentation (4.62 - 4.65)

The results of the review of all four designs, i.e. their safety claims, based on the provided documentation, using the Safety Requirements as identified in Reference 4, are documented in this report. The following section describes the project organization and conduct. Section 4 is organized into separate summaries of evaluation results for each reactor. At the project initiation it was agreed that presentation of IAEA's evaluation results would be aligned with HSE's reactor design assessment process. Therefore, IAEA safety assessment requirements were mapped in six major elements identified in HSE design assessment activities during Step 2 of the Design Acceptance and Licensing Process:

- (1) The safety philosophy and safety criteria used,
- (2) The design basis analysis/fault study approach,
- (3) PSA approach,
- (4) Overall scope of the safety case,
- (5) An overview of the claims in a wide range of areas of the safety analysis, and
- (6) Generic site envelope.

Each assessment summary in Section 4 is structured according to these six topics.

Attachments 1 through 4 provide a compilation of individual review sheets representing the consolidated view of the review team. The review sheets are organized according to Sections and Requirements paragraphs of the Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348" [4]. It is important to note that the IAEA review was conducted solely against the IAEA Safety Standards and not according to the HSE assessment approach. However, comments and observations by review team members may occasionally cite HSE criteria for purposes of clarification or for identification of their use by the Requesting Parties.

3. PROJECT ORGANIZATION AND CONDUCT

Given HSE's needs and the schedule laid out for the UK safety assessment of the proposed new reactors, the IAEA safety assessment review project had to be very compactly and efficiently organized and conducted. Due to this, a multifaceted review process was developed and implemented. Initially, the IAEA Division of Nuclear Installation Safety organized a team of external and internal experts to conduct the review of documentation provided by HSE within the available time period. The overall project management and coordination was provided by IAEA staff, and a team of international experts led by the IAEA management team conducted the evaluation against IAEA Safety Requirements. Technical leadership was assured by one of IAEA's senior external experts in consultation with IAEA staff. A secure web-based collaboration system was provided by the IAEA to the project as a platform to distribute and archive the documents to be reviewed, to collect and track review results and commentaries from the experts, and to provide a forum for announcements and discussions. The review work was conducted by the external experts at their base locations and only

two meetings of the review team were held at the IAEA: the first to initiate the project and the second to complete the review activities.

The implemented review process/methodology was focused on setting reliable measures to ensure that reviewers interpreted and applied the IAEA Safety Requirements in a consistent manner through expert meetings and teaming of external and internal experts by topic and other activities as discussed below.

First Experts Meeting

During the first meeting of the entire Review Team held in Vienna on 12-14 September 2007 the evaluation process and related Safety Requirements were discussed to gain a common understanding on the review concept and approach. This standard methodology for ensuring the necessary review consistency of approach included:

1. Group examination of each Safety Requirement [4] to compare and harmonize interpretations and applicability to the reactor design safety case being assessed, using critical judgement and technical expertise of the team.
2. Assignment of two or more experts to review the documentation against a specific set of IAEA Safety Requirements according to technical competence – each sub-team comprised of a principal reviewer and sub-reviewers – ensuring consensual and integrated analysis of each requirement addressed.
3. Enhancement of the above review process by teaming of both internal and external experts on each review topic to achieve a broader scope of assessment.
4. Pilot review and analysis by one of the reviewers of a proposed reactor design against two Requirements, which results were then presented to the Project Review Team for reflection and critique to enhance a unified review approach.
5. Formulation of standard language to be used in the review to ensure that each reviewer presented his or her analysis in a systematic and logical framework, providing a coherent set of results and comments for assigned portions of the review.

Internal Review and Screening by Project Team Leader & Managers

IAEA Project Managers electronically captured all inputs from each topical reviewer sub-team in a central database, the Centre for Advanced Safety Assessment Tools (CASAT), and reviewed all submissions to ensure the consistency and comprehensiveness of coverage by all reviewers on all topics. This screened content was released for comment to the entire project team as and when semi-final versions were received from reviewers.

Capturing Cross Cutting and Parallel Comments of Team Experts

The Review Team was tasked with scrutiny of all Requirements addressed by each consolidated sub-team review documented on the CASAT system, and to comment on, support or identify gaps in analysis submitted by the Sub-teams.

Final Review Team Meeting

The final review team meeting was held in Vienna from 5-7 November 2007 at IAEA Headquarters. All external experts, the IAEA project management team, and internal experts jointly discussed the review results as a whole and detailed points brought forward by the Team Leader for analysis. A representative from HSE joined the meeting to explain progress on the UK Design Acceptance and Licensing Process, and provide comments on the ongoing IAEA evaluation. Each lead reviewer was subsequently asked to provide revisions agreed by the team for their assigned Requirements. To ensure consistency, review team members were requested to submit input for the executive summary of the interim report according to the six major elements identified in HSE design

assessment activities outlined above. The work plan for the meeting was successfully concluded on 7 November 2007.

Consolidation of Results

The project management team subsequently consolidated the reviewers' inputs and prepared an interim report which included summaries of the review results for each reactor organized according to the six major elements identified in HSE design assessment activities during Step 2 of the Design Acceptance and Licensing Process. This interim report including the semi-final review results was provided to HSE for comments.

Final Report

After HSE comments were received, a meeting with HSE representatives took place in Vienna on 3-4 December 2007 to discuss the semi-final review results and agree upon modifications and changes to reflect HSE's comments. The interim report was subsequently edited and is now delivered to HSE as the final report.

Consideration of Additional Information on the ACR-1000

During the project review phase continuing contact with HSE was maintained. Additional information on the ACR-1000 was provided by the Requesting Party late in November and in early December, but was not considered during the initial review phase. Therefore, in accordance with a request from HSE, additional steps have been taken in the final stage of the project to consider this new information and to present an evaluation in the final report. It is recognised that although the ACR-1000 documentation was not sufficient to undertake a detailed assessment against the IAEA safety requirements, HSE requested only a preliminary safety report for Step 2 of its GDA and did not require detailed documentation of the safety case until Step 3 of the GDA in 2008.

4. SUMMARY OF REVIEW RESULTS

In the context of IAEA Safety Standards framework the review of the proposed four reactors proceeded using a bottom-up approach. Initially, the review was conducted against applicable Requirements, as discussed in the previous section, and secondly a general assessment was made to identify the adherence of the selected designs to the applicable Fundamental Safety Principles [2]. The evaluation identifies if the requirements are addressed in the design and safety documentation, and if evidence is provided supporting safety claims. The review does not address the correctness of technical claims made by the Requesting Parties. Also, the evaluation does not address specific details of compliance of the four designs to the IAEA design guidelines or specific details associated with safety analyses guidelines. The IAEA Safety Standards series of guidelines documents were considered in the review as supporting information only.

To align IAEA's evaluation with the HSE's Generic Design Assessment process, the review results are summarized in the following sub-sections according to elements in HSE's design assessment activities during Step 2 of the Design Acceptance and Licensing Process. We must stress here that the review was conducted strictly against IAEA Safety Standards, and that the alignment of the review results with HSE assessment activities is an editorial construct adopted purely for reporting convenience.

Safety philosophy and safety criteria

The IAEA examined the safety philosophy applied to, and the safety criteria used for demonstration of safety of the selected designs. Also, an evaluation was made of the extent to which the IAEA Safety Fundamentals [2] are addressed, including identification of application of defence in depth principles.

Principal IAEA Safety Standard used: Fundamental Safety Principles [2] Defence in Depth in Nuclear Safety [5], Assessment of Defence in Depth for Nuclear Power Plants [6], Safety of Nuclear Power Plants [3].

The design basis analysis/fault study approach

The provided documentation was reviewed to determine if design basis accidents are addressed, including the scenarios and conditions covered. Also consideration of severe

accidents, use of PSA in support of fault analysis, issues of model validation for deterministic and PSA studies was evaluated

Principal IAEA Safety Standard used: Requirements of Safety Assessment for Facilities and Activities [4].

PSA approach

The PSA methodology was reviewed in the context of IAEA Requirements.

Principal IAEA Safety Standards used: Requirements of Safety Assessment for Facilities and Activities [4]

Overall scope of the safety case

This review particularly focuses on assessing the extent to which the Requirements for a safety case are addressed by the Requesting Parties. A wide range of safety issues such as selection of initiating events, consideration of internal and external hazards, safety classification, design standards, quality assurance programmes and management approach, human factors, consideration of operational experience, etc. were considered.

Principal IAEA Safety Standards used: Fundamental Safety Principles [2], Requirements of Safety Assessment for Facilities and Activities [4], Safety of Nuclear Power Plants [3].

An overview of the claims in a wide range of areas of the safety analysis

The review evaluates whether the Requirements for safety analyses are addressed including consideration of uncertainties as well as availability of supporting information such as verification and validation of analytical methods.

Principal IAEA Safety Standards: Requirements of Safety Assessment for Facilities and Activities [4]

Generic site envelope

The review identified if demography, siting policies and criteria, external hazards such as seismic, flooding, meteorological, man made (except malicious), biological and geological were considered for a generic site envelope.

Principal IAEA Safety Standards used: Requirements of Safety Assessment for Facilities and Activities [4], Site Evaluation for Nuclear Installations [7].

The following Sections 4.1 through 4.4 summarize observations provided by the review team for each reactor design safety case, according to the six elements described above.

4.1 ACR-1000

This section summarizes results of the review of ACR-1000 documentation provided to the IAEA by HSE against IAEA Safety Standards, specifically “Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348” [4]¹. The review results summary is organized according to elements in HSE design assessment activities during Step 2 of the Design Acceptance and Licensing Process. The detailed results of the review are documented in Attachment 1 to this report². According to the terms of reference agreed by HSE and the IAEA for this assessment, work undertaken by the IAEA was based on design documentation which was publicly available on the 17th of September 2007. Although some additional information on the ACR-1000 design was provided by the Requesting Party late in November and in early December, it was not considered during the initial review phase. However, in accordance with a request from HSE, additional steps have been taken in the final stage of the project to consider this new information and to present it in the final report.

Limited documentation only was available for the review. The information provided consists of a Head Document ‘ACR-1000 Submission for Step 2 of UK Generic Design Assessment, Part I – HSE NII Requirements’. At the time of the review the Head Document was complemented by a long list of AECL documents, many at various stages of completion. They mainly contain the technical summary description of and the design philosophy, requirements, safety design guides and methodologies used for the ACR-1000 design. At this stage only limited results of safety analyses have been provided. At a later stage, more documents became available, a.o. describing more technical detail and some DBA-analyses.

The documentation was not sufficient to undertake a detailed assessment against IAEA safety requirements. However, it is recognized HSE asked at this stage only for a preliminary safety report and did not require detailed documentation of the safety case. Therefore, many features are projections or deductions based on past experience. However, the statements already provided in the submitted documents indicate in some detail the intentions of the ACR-1000 designers.

Safety philosophy and safety criteria

The ACR-1000 is largely based on existing CANDU technology, and safety principles of the ACR-700. Novel features are the use of enriched fuel and cooling by light water instead of heavy water. It is claimed that this results in a negative reactivity power feedback. In the design, both active and passive safety systems are used.

The iterative design process is summarized with reference to the development of the ACR-1000 as a long-term evolutionary process making use of the experience gained from the CANDU-900 and CANDU 6 designs. As part of the effort to demonstrate that the design is ALARP, the improvements made in comparison to the CANDU 6 are listed.

The ACR-1000 will be designed to meet the CNSC safety criteria. It is claimed that the design will address all Generic Action Items identified for CANDU reactors by the CNSC. AECL chose compliance with IAEA NS-R-1[3], and a detailed document has been prepared on how the NS-R-1 Requirements will be met by the design.

¹ The following thematic requirements groups were used for the review: Overall requirements for safety assessment (4.1 – 4.15); Assessment of the potential radiation risks (4.19); Assessment of safety functions (4.20 – 4.21); Assessment of site characteristics (4. 22 – 4.23); Assessment of radiological protection provisions (4.24 – 4.26); Assessment of the engineering aspects (4.27 – 4.37); Assessment of human factors (4.38 - 4.40); Defence in depth and safety margins (4.45 – 4.48); Scope of safety analysis (4.49 4.52); Approaches to safety analysis (4.53 – 4.56); Criteria for judging safety (4.57); Uncertainty and sensitivity analysis (4.58 – 4.59); Use of computer codes (4.60); Use of data from operating experience (4.61); Documentation (4.62 - 4.65).

² These review results are organized according to sections and requirements paragraphs of the Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348” [4].

Improvements affecting safety include a containment steel liner, modifications to the reactor assembly, strengthening of calandria tubes, replacement of both the liquid zone control and guaranteed shutdown liquid poison provisions with a rod-based system, change in header and feeder material, upgrades to the fuel handling and storage system, and upgrades to the control system.

Use of passive systems is planned for emergency core cooling, moderator cooling, reactor vault cooling and containment cooling.³

The safety system responses to design basis accidents are to be automated to the extent that no operator action is required for many hours after an initiating event.

High fuel burn-up is strived for as well as a plant life of 60 years. After 30 years of operation a complete replacement of the Pressure Tubes is foreseen.

The ACR-1000 has features to cope with severe accidents. Additional passive moderator and shield cooling is provided to prevent and mitigate fuel damage. It is intended to prevent core-concrete interaction. Hence, no provisions are in place to cope with non-condensables from the CCI. The technical basis for the CANDU severe accident mitigation is in part derived from the LWR technical basis.

It is claimed that the WENRA reference levels will be complied with. Regarding severe accidents it is claimed that the INSAG targets referred to in the IAEA standards will be met with a large margin.

It is claimed that all actual and potential sources of radiation are identified and properly considered. Design provisions are aimed at ensuring that sources are kept under strict technical and administrative control. Measures will be taken to ensure that occupational and public radiation doses will not exceed prescribed limits and are ALARA. Reference is made to the actual doses achieved at operating CANDU plants, which are below the design targets for ACR-1000.

Compared to earlier designs, the RP claims that the defence-in-depth concept is strengthened in the various levels. Aspects that may form part of the HSE assessment in Steps 3 and 4 could be to consider in detail aspects of increased burn-up and extended plant life, the technical basis of the mitigation of severe accidents, and the extrapolation from the ACR-700 design.

Design basis analysis/fault study approach

No detailed analysis of DBA treatment was presented. A list of postulated initiating events is provided. The 8 categories of PIE are grouped into AOOs, 2 categories of DBAs, and two categories of BDBAs. The 'Systematic Review of Plant Design for Identification of Initiating Events' will be available at a later stage.

It is reported that the design will address the single failure criterion, applying it to all active components at any time and to passive components for operation time longer than 24 hours.

A number of thermal-hydraulic analyses have been performed, some to serve the finalization of the design ('design assist analyses').

A PSA was not requested as part of the GDA Step2 documentation; it is planned to prepare a Level 1 and 2 PSA. It is indicated that the Level 2 PSA will consist of an assessment of potential

³ Frequent reference is made by requesting parties to passive safety systems which are not addressed in the IAEA Safety Standards. The IAEA Safety Glossary Pg. 140 definition for passive component is "a component whose functioning does not depend on an external input such as actuation, mechanical movement or supply of power".

bounding containment scenarios. Acceptance criteria and performance targets for 'Limited Core Damage Accidents' (LCDA) and 'Severe Core Damage Accidents' (SCDA) have been specified. LCDAs are defined as those in which the calandria stays intact. The Level 2 results will be interpreted to address risk based criteria.

PSA approach

The documentation includes procedures for conducting Level 1 and 2 PSA, containing considerable detailed information with some particular references to CANDU designs. In addition to the processes, methods, and techniques to develop a PSA, the documents refer to the probabilistic safety targets that the design will have to meet. Since Level 3 PSA is neither a requirement nor a common practice in Canada, the intention for the UK licensing submissions is to interpret the Level 2 PSA to address the Level 3 (risk) based safety criteria specified in the SAPs.

Some results from the ACR-700 PSA are provided. The Requesting Party indicates that the ACR-1000 will result in still lower severe accident frequencies exceeding the INSAG targets referred to in the IAEA Safety Standards by approximately two orders of magnitude.

Overall scope of the safety case

The full safety case has not as yet been submitted. The Requesting Party was asked to submit a "Preliminary Safety Report" to include sufficient information for the Step 2 Fundamental Safety Overview. Reference is made to the limited design review of the ACR-700 by the NRC and the pre-licensing review of the ACR-1000 by the CNSC, which was not fully completed.

Reference is also made to the long operating experience with several generations of CANDU designs over the last 30 years. The RP has implemented a Feedback Monitoring System which captures operational experience feedback aimed at ensuring that the issues are addressed in future designs.

A particular feature of CANDU reactors is on-power refuelling. Inadvertent loading and operation of a fuel bundle in an improper position and fuelling machine related events are included in the design basis events. It is indicated that such events will be included in the PSA when details of the fuelling machine design and operation are known. More information will be provided by the RP on how refuelling related events have been analysed in later steps of the GDA.

Overview of the claims in a wide range of areas of the safety analysis

More information is needed on the methodology to confirm that the design includes sufficient margins to cater for process parameter variations, process parameter uncertainty measurements, analysis uncertainties and maintenance activities.

The technical basis for the criteria used in the thermal hydraulic analysis should be provided and the assumptions used in the thermal hydraulic analyses need to be further evaluated in the next steps of the GDA process.

As the margin to the criteria sometimes is small (peak sheath temperature 1180 °C, where the assumed limit is 1200 °C), more evidence should be provided about the conservatism of the calculation, or appropriate uncertainty analysis should be provided. In addition, it is not clear whether multi-channel effects have been sufficiently incorporated.

Some thermal hydraulic analyses predict large temperature transients, e.g. large cool down rates. No analysis has been provided that this is inside the mechanical capabilities of large components, such as headers and steam generators (notably the tube sheet). The detailed assessment should include these structural analyses.

Regarding the relocation of core debris into the calandria vault, more information should be provided on an analysis of the phenomena related to this accident sequence, after the ACR-

1000 layout has been finalized. In particular the modelling of the spreading of the debris and the development and validation of the related computer codes should be documented.

Substantial margin is claimed to be included in the ACR-1000 design to address the level of uncertainties associated with the current validation base.

As part of the development of the PSA, uncertainty analyses will be performed on parameters such as failure rates, component unavailabilities, initiating events, and human error probabilities. Sensitivity analyses will test the impact of certain changes in key input values.

Uncertainty elements will be categorized as natural randomness of a quantity and as lack of knowledge of a quantity.

The ACR is an evolution from the proven CANDU 6 design. Therefore, only a few computer codes required modifications and experimental data base extensions consistent with the different operating conditions of the ACR-1000 (mainly higher pressure, higher temperature, higher enrichment, and the use of light water coolant). A software quality assurance programme is in place.

Addressing the relevant IAEA Safety Requirements established in NS-R-1, plant-specific safety functions have been derived from the three Fundamental Safety Functions. An additional Fundamental Safety Function has been included: "Monitor critical safety parameters to guide operator action". The safety functions will be achieved for normal operation modes (including start-up and shut-down), all AOO and accident conditions.

The safety classification scheme of SSC is based on the safety importance of the function of the SSC. The safety classification method considers the consequences of failure to perform the function of an SSC and the time following a PIE. More information should be provided on how the probability that the SSC will be called upon has been considered.

Most of the SSC were allocated to the safety classes but at this stage of the design this is not finalized. More information should be provided on how the classification of the software for I & C will be performed.

A number of systems are classified as non-safety, which may still be relevant for safety seen from the defence-in-depth principle. For example, systems that mitigate beyond design basis events have relevance for safety, but are classified class D, i.e. commercial grade. Others may not formally have a role in mitigating possible releases, but protect important fission product boundaries (e.g. role of containment spray in steam line break accident).

In the matter of pressure boundary integrity, isolation devices between different classes may not always have the proper safety weight (e.g. one isolation valve, where two are common).

The next step safety assessment should address the classification in detail, and should notably address the systems which are classified non-safety, as well as the proper classification for interfaces of pressure retaining components.

Generic site envelope

A generic site envelope is provided for the ACR-1000 that identifies natural and human induced hazards that have the potential to affect the plant. Natural external hazards include extreme weather, earthquake and external flooding. Man-made hazards include aircraft crash, transportation and industrial activities (fire, explosion and toxic gases). The documents specify requirements for site-specific evaluation once a plant location is selected. The ACR-1000 will be designed to an AECL standard ground motion spectrum anchored to 0.3g peak ground acceleration.

Airplane crash is addressed as part of site selection with reference to the modern international requirements on aircraft impact design.

The procedures for selecting the site and identification and evaluation of hazards follow accepted industry practice and address the IAEA Requirements for Nuclear Power Plants (NS-R-3, NS-G-3.1, 1.5, 3.4, and 3.5). The generic site envelope is provided in ACR108-10100-PPS-001. If a UK site falls outside this envelope, AECL will perform some limited design modification or conclude that the site is not suitable.

The IAEA Requirements are generally addressed. A list of the external hazards to be assessed is provided.

The PSA to be provided for external events should include a PSA based Seismic Margin Assessment. The aim is to show a seismic margin of 0.50g peak ground acceleration for the standard plant. Seismic design of the plant will follow the Safety Design Guide-002. Tornado design will be based on Safety Design Guide -008, which may be overly conservative for UK sites.

Based on the review of the provided documentation it appears that the ACR-1000 is being designed to the applicable IAEA Fundamental Safety Principles. However, since the documentation is limited at this stage, it was not possible to assess, for many of the IAEA Requirements, if they are or will be addressed. Key issues requiring further detailed review or more evidence and information were identified and are briefly described in the summary of review results above. These are issues that the HSE may take up as part of their assessments undertaken in GDA Steps 3 and 4. These issues are discussed in greater detail in the individual review sheets provided in Attachment 1.

4.2 AP1000

This section summarizes results of the review of AP1000 documentation provided to the IAEA by HSE against IAEA Safety Standards, specifically “Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348” [4] *. The review results summary is organized according to elements in HSE design assessment activities during Step 2 of the Design Acceptance and Licensing Process. The detailed results of the review are documented in Attachment 2 to this report**.

Detailed documentation was available for the review. It consisted of a set of documents ‘UK Compliance Document for AP1000 Design’ specifically aimed at addressing the requirements of the UK HSE Step 2 request. This set included a ‘Safety Assessment Roadmap for AP1000 design’, a ‘Western European Nuclear Regulator’s Association Roadmap’ and the ‘NRC AP1000 Final Safety Evaluation Reports’. This set of ‘Head Documents’ is complemented by detailed safety analyses contained in the ‘UK AP1000 Safety, Security, and Environmental Report’.

The analyses presented follow the US NRC procedures and are documented in the standard DCD format. The Head Documents provide precise guidance on where more detailed information and results of relevant analyses are provided in the DCD. In addition the documentation included the ‘UK AP1000 Probabilistic Risk Assessment’.

Safety philosophy and safety criteria

The AP1000 is an extrapolation of an earlier design (AP600), and makes extensive use of new technology compared to the fleet of operating Westinghouse PWRs, e.g. a passively cooled containment system, canned RCPs connected to the SGs, a depressurization system for SBLOCA-events, and passive ECCS.

The iterative process leading to the AP1000 design is documented. The AP600 design was strongly influenced by the results of various PSA studies and was developed concurrently with the US Utility Requirements Document (URD). Therefore, the safety philosophy is based on the US URD for passive designs also placing more reliance on increased thermal margins. Components for power production are mainly of a proven design of the fleet of Westinghouse PWRs built earlier; however, decay heat removal and emergency core cooling consist of innovative passive and simplified safety systems.

The leak-before-break concept has been applied to RCS pipes greater than or equal to 4 inches diameter. Through selection of materials and manufacturing processes stresses could be reduced, thus reducing the chance of cracking and reactor coolant leakage or LOCA accidents. In spite of the fact that this results in SBLOCA being a very low probability event, high pressure injection has been retained. High pressure injection is provided by a core make-up tank, entirely passive and capable of injecting at full core pressure. Also the capability to mitigate LBLOCA has been retained in the design basis.

No operator action is required for mitigating design basis events for many hours after the initiation of the event.

* The following thematic requirements groups were used for the review: Overall requirements for safety assessment (4.1 – 4.15); Assessment of the potential radiation risks (4.19); Assessment of safety functions (4.20 – 4.21); Assessment of site characteristics (4. 22 – 4.23); Assessment of radiological protection provisions (4.24 – 4.26); Assessment of the engineering aspects (4.27 – 4.37); Assessment of human factors (4.38 - 4.40); Defence in depth and safety margins (4.45 – 4.48); Scope of safety analysis (4.49 4.52); Approaches to safety analysis (4.53 – 4.56); Criteria for judging safety (4.57); Uncertainty and sensitivity analysis (4.58 – 4.59); Use of computer codes (4.60); Use of data from operating experience (4.61); Documentation (4.62 - 4.65).

** These review results are organized according to sections and requirements paragraphs of the ‘Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348’ [4].

Basic design objectives are a plant life of 60 years and high fuel burn-up.

The design includes features to cope with severe accidents, where the philosophy is to keep the debris inside the vessel and remove decay heat via a passive containment cooling system. Hence, no provisions are in place to cope with non-condensables (except for hydrogen) from the CCI.

The technical basis for the severe accident mitigation is based on extrapolations from the AP600 design.

The novel safety features are aimed at early core depressurization in case of severe accident scenarios, prevention of containment bypass through main steam line break, and keeping the containment intact throughout the accident. Passive containment cooling is to be assured by the combination of a large water reservoir providing cooling in the initial phase of the accident and natural circulation of outside air to remove heat from the containment in the long term.

The safety criteria used are the NRC requirements for all events up to and including DBA, and NRC safety goals for BDBA, including severe accidents safety goals, e.g. intact containment for at least 24 hours after onset of core damage and no more than 0.1 conditional containment failure probability.

ALARA is applied in controlling the exposure of the workers and of the public. The materials, plant layout, chemistry, and maintenance work minimization are designed so as to make radiation exposures as low as reasonably practicable.

Compared to earlier designs, the defence-in-depth concept is strengthened in the various levels, provided the various claims of the Requesting Party can be confirmed in further assessments. Therefore, there is the need in the further review to consider in detail aspects of increased burn-up and extended plant life, the technical basis of the mitigation of severe accidents, and the extrapolation from the AP600 design to the AP1000.

Design basis analysis/fault study approach

The transients and design basis accidents are considered according to NRC guidelines. Internal and external hazards are addressed. Depressurization is an important safety feature, aimed at preventing high pressure core melt scenarios by using highly redundant and diverse automatic depressurization valves. Retaining molten corium inside the vessel prevents corium/concrete interaction and steam explosions from challenging the containment. Hydrogen detonation is to be prevented by using a large rugged containment vessel, igniters and passive autocatalytic recombiners.

Melt arrest and containment integrity are claimed to be achieved by cooling the outside of the RPV. Better evidence should be provided that the experimental and analytical results gained for the AP600 will also apply to the AP1000 and the consequences should be assessed if the melt arrest within the RPV was not successful.

In general, the AP1000 design uses redundancy features to deal with single failure criteria, diversity is used to address shutdown requirements, and segregation is used to account for fire, flood and seismic requirements.

It is claimed that due to the novel design features, such as the passive safety systems, containment spray is judged not to be required and there is also no requirement for safety related emergency AC power based on the safety classification system used in the US.

Further evidence should be provided to allow assessment of the performance of the novel passive functions - emergency core cooling and decay heat removal - and the scaling from experimental size of these features to the AP600 and then to the AP1000.

The Level 1, 2 & 3 PSA including external events and shut-down risk (hot/cold shutdown and mid-loop conditions) has been performed to optimize the design and to demonstrate compliance with the US NRC safety goals.

PSA approach

The documentation includes a systematic probabilistic safety analysis of the AP1000 design making use of the results of the PSA prepared earlier for the AP600. Level 1, 2 and 3 analyses have been performed for internal initiating events. Low power and shutdown operational states are analysed only in the Level 1 PSA. The Level 3 PSA is limited to an off-site dose evaluation.

The scope of hazards considered is limited to internal floods, fires and earthquakes (seismic margin assessment). External hazards, such as tornadoes, hurricanes, external floods and transport accident are addressed but excluded from the analysis on the basis that the plant site should be such that the frequency of such hazards with a magnitude sufficient to challenge the safety of the plant is below $1E-6$ /reactor-year. There is the need in the further review to consider in detail the screening of external hazards to address site specific characteristics.

The PSA was presented with the application for design certification by the US NRC. It claims to be in compliance with the US NRC safety goals with significant margins and presents a balanced risk profile. Some parts of the PSA make use of the results of the AP600 PSA or are developed from the models of the AP600 PSA with some considerations of design differences. Therefore, there is the need in the further review to consider in detail to which degree the similarity of both designs allows extrapolating the results or models of the safety assessment for the AP600 to the AP1000.

Overall scope of the safety case

Following the standard DCD format the selection and grouping of anticipated operational occurrences and accident conditions within the design basis follows the standard US NRC procedure. Safety analyses are based on a deterministic approach complemented by probabilistic methods.

Reference is made to the long operating experience with the fleet of reactors based on Westinghouse technology. A list of design improvements is given to demonstrate the use made of the US utilities formal process to collect operating experience leading to the US URD and of the similar European efforts.

An evaluation of radiation doses for all accident conditions is given, including radiological releases and radiation doses after severe accidents. The respective accident analyses follow the standard US NRC procedure based on a classification of plant conditions into 4 categories.

Information is provided on how the results of safety analyses described in the DCD and the PSA, aimed at demonstrating compliance with the NRC criteria, address the SAPs of the UK HSE. It is claimed that the AP1000 design has addressed all relevant UK SAPs in sufficient detail. In addition information is provided on how the AP1000 design compares to the WENRA safety reference levels, the US Advanced Light Water Reactor Utility Requirements (URD) and the European Utility Requirements (EUR).

The AP1000 has undergone the US NRC design certification process. The NRC Final Safety Evaluation Report for the AP1000 Design was included in the documentation. It is claimed that there are no open items.

Due to the way that the AP1000 accomplishes safety related functions through passive systems it is indicated that an adaptation of the safety classification system based on the US industry standards and regulatory guides had to be made.

The classification system does not explicitly address the relevant Requirements as formulated in IAEA 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 AP1000 is implicitly addressing the IAEA Requirements and the SAPs.

Overview of the claims in a wide range of areas of the safety analysis

Important features for severe accident mitigation are based on both a theoretical and experimental basis and on an extrapolation from the AP600 design. The latter involves phenomena which might be insufficiently known to allow for high reliability of scaling. This includes external vessel cooling of molten corium, with uncertainties concerning both corium stratification and coolability in a large vessel and the effectiveness of cooling by natural circulation of water outside the bottom cover of a large size vessel. In view of the involved uncertainties, better evidence should be provided that the systems will protect the containment in case the external vessel cooling turns out to be insufficient to prevent vessel melt through.

Uncertainties (statistic and deterministic) are included in the core layout, stability analysis, scale-up considerations, etc. There is the need in the further review to consider in detail their potential systematic deviation and propagation during the transients and consequences on the results of the safety analysis for DBA and BDBA sequences. In this regard, the high burn-up behaviour under DBA transients is a relevant safety issue (code validation, methodology, criteria).

The computer codes used for analysing the behaviour of the novel features (emergency core cooling and decay heat removal) are the existing well-known codes, except for the codes modelling the melt arrest within the RPV. More evidence should be provided regarding the application and validation of these codes to the AP1000, including assessment of hydrogen behaviour and the effects of additional non-condensables.

Generic site envelope

The designer has developed the generic site envelope for the AP1000 that describes the natural and human induced hazards covered under the site parameters. An actual site is acceptable if its site characteristics fall within these site design parameters.

The quantitative criteria to be used for selecting the design basis hazards are described. In addition to earthquakes, tornado and external flooding, the following human induced hazards will be evaluated for a particular site: explosions, flammable vapour clouds, toxic chemicals, fires and airplane crashes. The UK requirements on Regulatory Assessment of Siting ST1, ST2 and ST3 are addressed. (However, the UK requirements do not define a margins event.) It is also shown to meet the applicable USNRC regulatory guides.

The Safe Shutdown Earthquake for the Standard Plant is reported as 0.3g peak ground acceleration which exceeds the typical SSE level plants in the UK (0.25g). Further the seismic margin goal for the plant is 0.5g which is also larger than the typical level in the UK (0.35g).

Following the EUR, AP1000 NPPs will be designed to withstand the impact of a postulated aircraft. For UK application AP1000 designers have committed to provide a containment design that will be capable of withstanding an aircraft crash without a significant impact on the public health and safety.

Based on the review of provided documentation it appears that the AP1000 design conforms to the applicable IAEA Fundamental Safety Principles. The review also indicates that the safety case is presented in a level of detail which allowed assessing in most cases if the IAEA Requirements have been addressed. Several issues requiring further detailed review or more information were identified and are briefly addressed in the summary of review results above. These issues are discussed in greater detail in the individual review sheets provided in Attachment 2.

4.3 EPR

This section summarizes results of the review of EPR documentation provided to the IAEA by HSE against IAEA Safety Standards, specifically “Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348” [4]*. The review results summary is organized according to elements in HSE design assessment activities during Step 2 of the Design Acceptance and Licensing Process. The detailed results of the review are documented in Attachment 3 to this report**.

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

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

Safety philosophy and safety criteria

The EPR is an evolutionary design based on existing French and German designs. A number of new features have been added and some of the features available in the existing designs, in particular the HPSI, have been removed. The EPR uses both active and passive safety systems.

The iterative process is summarized by making reference to the long list of IRSN review reports since April 1992. They document the process of French and German co-operation leading to the EPR design. The EPR basic design took into account French and German safety requirements, the European Utility Requirements (EUR) and the requests of French and German utilities. Components for power production and heat removal are of proven design from a fleet of operating French and German reactors. The results of the PSA have been used in an iterative process to provide features aimed at preventing or mitigating core damage resulting from multiple failure conditions (Risk Reduction Categories RRC-A and RRC-B)

An important aspect is the ‘break preclusion’ concept, which has removed the LBLOCA from the ECCS design basis. However, LBLOCA has been maintained as the design basis for the containment. Due to the RP claims of a more favourable design of the reactor pressure vessel which reduces the extent of core uncovering in the case of the small LOCA, it has been possible to reduce the injection pressure of the HPSI (now referred to as the MHSI) below the SG safety valve set point, achieving a reduction in SG overfill risks compared to existing plants and avoiding the risk of liquid discharge through the safety valves.

* The following thematic requirements groups were used for the review: Overall requirements for safety assessment (4.1 – 4.15); Assessment of the potential radiation risks (4.19); Assessment of safety functions (4.20 – 4.21); Assessment of site characteristics (4. 22 – 4.23); Assessment of radiological protection provisions (4.24 – 4.26); Assessment of the engineering aspects (4.27 – 4.37); Assessment of human factors (4.38 - 4.40); Defence in depth and safety margins (4.45 – 4.48); Scope of safety analysis (4.49 - 4.52); Approaches to safety analysis (4.53 – 4.56); Criteria for judging safety (4.57); Uncertainty and sensitivity analysis (4.58 – 4.59); Use of computer codes (4.60); Use of data from operating experience (4.61); Documentation (4.62 - 4.65).

** These review results are organized according to sections and requirements paragraphs of the “Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348” [4]

Basic design objectives are a plant life of 60 years and high fuel burn-up.

No operator action is required for mitigating design basis events for at least 30 minutes after the initiation of the event.

The design includes features to cope with severe accidents. The philosophy is to prevent high pressure core melt accidents and to protect the containment integrity in case of low pressure severe accidents. In-vessel cooling is not considered to be effective for the EPR power level; therefore, a core retention system below the RPV has been developed. The philosophy is, following low pressure vessel rupture, to arrest the melt after spreading in a dedicated area. The debris is then cooled by an overlying water pool with water supplied from the IRWST. By providing sacrificial material and basemat cooling the system is designed to prevent core-concrete interaction. Therefore, intentional containment venting is not included in the design. Hydrogen is mitigated by passive autocatalytic recombiners. A dedicated depressurisation system is aimed at preventing high pressure paths of severe accidents.

The safety criteria used are the requirements of the EPR Technical Guidelines (TGs), which resulted from the process of French and German co-operation with international participation. The TGs are deterministic in nature and do not estimate individual risk or demonstrate that risks are ALARP. A novel feature is the requirement to 'practically eliminate' large early releases. This concept is also referred to in the IAEA Safety Standards.

As a result of the application of this philosophy and the EPR TG's criteria, it is claimed that the radiological effects of a severe accident with core melt are reduced to a level which will not necessitate any long term restrictions in food production or population evacuation. The core melt and large release frequencies are estimated to be well below the INSAG target values referred to in the IAEA Safety Standards.

ALARA is applied in controlling the exposure of the workers and of the public. The materials, plant layout, chemistry, and maintenance work minimization are designed so as to make radiation exposures as low as reasonably practicable.

Compared to earlier designs, the defence-in-depth concept is strengthened in the various levels, provided the various claims of the Requesting Party can be confirmed in further assessment. There is the need in the further review to consider in detail the 'break preclusion' concept, aspects of increased burn-up and extended plant life, areas where safety systems of earlier designs have been removed, and the technical basis for the mitigation of severe accidents.

Design basis analysis/fault study approach

The transients and design basis accidents are considered according to the EPR TGs and EUR guidance. Internal and external hazards are considered. Depressurization is an important safety feature. It is claimed that it significantly reduces containment bypass hazard. However, this approach to safety functions led to the removal of the HPSI. Studies and validation of measures used to cope with over pressurization hazards are described and should be reviewed in detail at the next step.

No attempt is made to provide external cooling of the reactor pressure vessel in case of core melt. Rather the concept of corium control relies on a dry core melt retention system to prevent steam explosion and to assure thin spreading of the hot corium to allow for its subsequent cooling. The concept of a core melt retention system has been developed based on experimental results for hot corium. Therefore, design measures are aimed at assuring that the corium will be hot at the moment of relocation into the retention system. The evidence provided for the performance of the melt retention system should be reviewed in detail at the next step.

The design provides for increased redundancy, diversity and separation, improved man-machine interface and extended response time for operator action.

PSA Level 1+ has been used systematically as a tool to identify severe accident sequences and to optimize design features aimed at reducing their contribution to overall risk. It is planned to prepare a full-scope Level 1, 2, 3 PSA for the Pre-Construction Safety Report.

PSA approach

A PSA Level 1+ has been performed at this stage. It covers internal initiating events and internal and external hazards in all operational modes. Due to the break preclusion concept, 2A LOCA and 2A SLB accidents (between the SGs and the fixed points downstream of the MSIVs) are "considered sufficiently low not to require consideration in the PSA".

From the PSA results, risk reduction categories were elaborated for reducing the importance of relevant risk contributors. In particular the objective of the reduced scope Level 2 PSA has been to perform a quantification of the 'early containment failures'. In conjunction with deterministic arguments, it was used to demonstrate their 'practical elimination' in compliance with the EPR TGs.

The PSA has been carried out during the design process in accordance with French regulatory requirements. The use of PSA for improving the design is summarized with the objective to demonstrate that the design is ALARP.

A summary only of the PSA is included in the documentation. Therefore, little information is provided on the PSA methodological aspects and on particular areas of the PSA, e.g. analysis of low power and shutdown operation and analysis of hazards. Therefore, there is the need in the further review to consider in detail the PSA based on more detailed PSA documentation, including the elimination of 2A LOCA and SLB from the list of initiating events.

Overall scope of the safety case

The selection and grouping of anticipated operational occurrences and accident conditions within the design basis follows the EPR TGs. The 2A LOCA is eliminated due to the break preclusion concept. However, the experience from RCS piping construction of the Olkiluoto 3 NPP in Finland has not been discussed.

The process of making use of the long operating experience is documented. It is stated that the decision to follow an evolutionary design had the advantage of basing an advanced design on the operational experience from a large fleet of reactors constructed by Framatome and Siemens. In addition the national operating experience collected by the US NRC and the international experience collected by the IAEA have been utilized.

Based on the experience with earlier similar reactors an evaluation of radiation doses for normal operation is provided. The radiological consequences of design basis accidents are estimated making use of standard computer codes. Since a Level-3 PSA is not yet available, dose estimates have not yet been provided for the analysed 3 plant damage states.

Information is presented on a comparison of the EPR design to the WENRA reference levels. Experience from the licensing reviews by the French and the Finnish Regulator is summarized. A comparison with the revised EUR has recently been launched.

Addressing the Requirements of IAEA NS-R-1, SSCs have been classified on the basis of their function and significance with regard to safety. Plant-specific safety functions have been identified in order to achieve the three Fundamental Safety Functions. Information is provided on how these safety functions can be performed for normal operation modes (including start-up and shutdown), all AOO and accident conditions.

The safety classification method considered the consequences of failure of the SSC to perform its function, the time following a PIE and time period it will be called upon to operate. Further evidence should be provided that the probability that the SSC will be called upon to perform a safety function has been included in the considerations for classification.

Most of the SSC have been allocated to safety classes but at this stage of the design the classification is not yet finalized. More evidence should be provided regarding the classification system of the software for I&C equipment.

Overview of the claims in a wide range of areas of the safety analysis

Important features for severe accident mitigation are based on both theoretical and experimental evidence. Notably much work has been done in the area of prevention of early containment failure.

The melt retention concept is based on extensive experimental work and numerical analysis. However, the random character of core melt processes requires careful consideration and means should be available to protect the containment in case of deviations from the assumed scenarios. Given the uncertainties related to the scenarios of core melt propagation for severe accidents, there appears to be a need to address, in the further review, the evidence provided that containment venting at full pressure is not required.

The design includes measures to prevent certain accidents from occurring. As a consequence the systems designed for coping with such accidents have been removed. The justification of this approach would need to be reviewed in detail at the next step.

Uncertainties (statistical and deterministic) are included in the core layout, stability analysis, and scale-up considerations, etc. There is the need in the further review to consider in detail their potential systematic deviation and propagation during the transients and consequences on the results of the safety analysis for DBA and BDBA sequences.

The codes to be used for DBA and BDBA sequences have been used for existing designs except those related to hydrogen behaviour and melt arrest. Much R&D work has been performed including related experiments and computer code developments.

Generic site envelope

A Generic Site Envelope has been developed for the EPR. Potential natural (i.e., earthquakes, flooding, meteorological, biological and geological) and human induced hazards (i.e., aircraft impact, explosions, and missiles) typically considered in the NPP design have been addressed. Since these hazards are considered site-specific, information is provided on how these have been evaluated for Flamanville-3 with indications on how it will be applied to a UK site.

The EPR seismic design spectrum is defined as “ EUR scaled to 0.25 g” and is designed to envelope nine ground conditions. If a future UK site condition is outside this range additional analyses will be needed.

The seismic risk of core damage is shown to be low for the Flamanville EPR based on the stringent seismic design. Therefore, a seismic margin assessment as is typically done for standard plants where a specific site is not known in advance is not discussed. The demography around the potential UK nuclear sites is evaluated. It is claimed that emergency planning and siting policy criteria have been met by this reactor design.

The protection against aircraft crash is an “aircraft shell” for buildings containing nuclear fuel and either sufficient geographical separation between redundant systems or an “aircraft shell” for buildings with essential safety equipment.

Based on the review of provided documentation it appears that the EPR design is in line with the applicable IAEA Fundamental Safety Principles. The review also indicates that the safety case is presented in a level of detail which allowed assessing in most cases if the IAEA Requirements have been addressed. Several issues requiring further detailed review or more information were identified and are briefly addressed in the summary of review results above. These issues are discussed in greater detail in the individual review sheets provided in Attachment 3.

4.4 ESBWR

This section summarizes results of the review of ESBWR documentation provided to the IAEA by HSE against IAEA Safety Standards, specifically “Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348” [4]*. The review results summary is organized according to the elements in HSE design assessment activities during Step 2 of the Design Acceptance and Licensing Process. The detailed results of the review are documented in Attachment 4 to this report**.

Detailed documentation was available for the review. The Head Document ‘ESBWR – UK Preliminary Safety Report’ is specifically aimed at addressing the requirements of the UK HSE Step 2 request. It is complemented by the safety analyses contained in the ‘ESBWR Design Control Document’.

The analyses presented follow the US NRC procedures and are documented in the standard DCD format. The Head Document provides precise guidance on where more detailed information and results of relevant analyses are provided in the DCD. However, in a few cases the detailed analyses were not yet available.

Safety philosophy and safety criteria

The ESBWR is an evolutionary design based on design features of operating BWRs. Novel features include the natural circulation within the vessel for power production and the extensive use of passive systems for heat removal and emergency cooling to cope with design basis accidents.

The iterative process leading to the ESBWR design is documented. The safety philosophy of the design is based on the US Utility Requirements Document (URD), which places a.o. more reliance on passive safety systems and has increased thermal margins. Many components are based on proven design of the fleet of GE BWRs built in the past. However, some of the systems available in those earlier designs have been taken out, in particular the capability to inject water at high pressure.

No information could be found in the documentation regarding the application of the leak-before-break concept. The containment design does not consider or utilize leak-before-leak applicability with regard to protection against dynamic effects associated with a postulation of rupture in high-energy piping.

Resolution of intersystem LOCA hazards takes into account the recommendations of NRC staff concerning detection of possible leakages. Low pressure systems have been strengthened to provide a reasonable protection against burst failure should the low pressure system be subjected to full RCPB pressure. Thus the design pressure of low pressure piping that interface with RCPB is equal to 0.4 times the normal operating RCPB pressure.

No operator action is required for mitigating design basis events for many hours after the initiation of the event.

Basic design objectives are a plant life of 60 years and high fuel burn-up.

* The following thematic requirements groups were used for the review: Overall requirements for safety assessment (4.1 – 4.15); Assessment of the potential radiation risks (4.19); Assessment of safety functions (4.20 – 4.21); Assessment of site characteristics (4. 22 – 4.23); Assessment of radiological protection provisions (4.24 – 4.26); Assessment of the engineering aspects (4.27 – 4.37); Assessment of human factors (4.38 - 4.40); Defence in depth and safety margins (4.45 – 4.48); Scope of safety analysis (4.49 4.52); Approaches to safety analysis (4.53 – 4.56); Criteria for judging safety (4.57); Uncertainty and sensitivity analysis (4.58 – 4.59); Use of computer codes (4.60); Use of data from operating experience (4.61); Documentation (4.62 - 4.65).

** These review results are organized according to sections and requirements paragraphs of the Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348” [4]

The design includes features to cope with severe accidents, where the philosophy is to keep the debris inside the vessel by external flooding. Hence, no provisions are in place to cope with non-condensables from the CCI in case the exterior vessel cooling is not successful. In order to mitigate such accidents the Basemat Internal Melt and Coolability Device (BiMAC) has been added, which has been developed at the conceptual level only. Hydrogen risk has been mitigated by permanent inertion.

The safety criteria used are the NRC requirements for all events up to and including DBA, and the NRC safety goals for BDBA, including severe accidents safety goals, e.g. intact containment for at least 24 hours after onset of core damage and no more than 0.1 conditional containment failure probability.

Information is provided on how occupational and public radiological risks are being controlled within the principles, targets, and legal limits specified by the SAPs of the UK HSE. ALARA assessments are reported for controlling occupational exposure. Public radiological exposure is considered ALARA if the acceptable dose limits specified by the US NRC are met. Regarding prevention or mitigation of severe accidents SAMDA analyses are presented to assess the cost-effectiveness of additional measures to enhance safety.

Compared to earlier designs, the defence-in-depth concept is strengthened in the different levels, provided the various claims of the Requesting Party can be confirmed in further assessment. Therefore, there is a need to give particular attention in further reviews to the assessment of the stability of the natural circulation, to areas where safety systems of earlier BWR-designs have been removed, to aspects of increased burn-up and extended plant life, and to the technical basis for the mitigation of severe accidents.

Design basis analysis/fault study approach

A system level qualitative Nuclear Safety Operational Analysis (NSOA) methodology is used to systematically obtain the list of events and applicable plant operating modes which have been included in the DBA analysis. Waste gas system leaks or failure are considered.

The underlying fault studies to support severe accidents by exterior cooling of the RPV and the melt arrest (BiMAC) were not presented with the submission.

In general, the ESBWR design addresses requirements for redundancy, independence of redundant systems, diversity and resistance to single failures.

The ESBWR natural circulation and the passive safety systems are significantly simpler than those for previous designs because they contain significantly fewer components and thus require fewer tests, inspections and less maintenance. In addition, no AC power to operate safety related equipment is needed, based on the safety classification system used. Nevertheless, these novel features necessitate further evidence because experiments and results from former operating plants have to be scaled-up.

Only a brief summary of the PSA is included in the documentation. It is noted that in spite of bounding assumptions 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 internal events LRF (in the range of $1 \text{ E-9}/\text{reactor-year}$) are very low. Level 2 and 3 PSA results will strongly depend on the reliability of outside cooling of the RPV and the performance of the BiMAC. Therefore, the PSA should be reviewed in detail at the next step.

PSA approach

The detailed PSA report NEDO-33201 was not available for the review. From the brief summary information provided it can be concluded that with some limitations the PSA covers Level 1, 2, and 3 for internal initiating events, external hazards and all modes of operation.

The PSA is largely based on bounding approximations and generic data. Limited information is provided on the risk contributors, the methods applied, generic data used and the use of bounding assumptions when reliable information is not available. The limitations for performing

a PSA during the design process are recognized. The fire and flood analysis will need information on the routing of cables and piping.

The Level 3 PSA is not described. However, it is claimed that the safety goals are met with a very large margin. This conclusion will depend on the results of the analyses of the provisions to address severe accidents. The very low risk results obtained with bounding and conservative analyses require a detailed review.

Overall scope of the safety case

Following the standard DCD format the selection and grouping of anticipated operational occurrences and accident conditions within the design basis follows the standard US NRC procedure. Safety analyses are based on a deterministic approach complemented by probabilistic methods.

Reference is made to the use of the long reactor operating and testing experience of similar nuclear power plants obtained from NRC Licensee Event Reports, INPO correspondence and through other industry sources.

The accident analyses follow the standard US NRC procedure and cover normal operation, anticipated operational events, infrequent events, design basis accidents, special events, and beyond design basis accidents. Estimates for radiation doses for all accident conditions are provided, including radiological consequences of severe accidents.

Information is provided on how the safety objectives and criteria established by the US NRC are addressed. Summary information is provided on how these relate to the UK HSE requirements; however, it is indicated that further analyses will be needed to demonstrate clearly this relation.

The DCD includes a detailed list of the regulatory and industry standards used. The ESBWR design is undergoing the design certification process of the US NRC.

Because of specific design considerations, it is indicated that the general definitions in US industry codes and standards for safety classification are subject to interpretation and exceptions. Information is provided on design requirements for SSCs commensurate with the safety-related functions to be performed.

The classification system does not explicitly address the relevant Requirements as formulated in IAEA 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 what extent the classification system used for the ESBWR implicitly addresses the IAEA Requirements and the SAPs.

Overview of the claims in a wide range of areas of the safety analysis

The design includes novel passive features to cope with severe accidents. It is claimed that the ESBWR is designed to minimize the effects of direct containment heating, ex-vessel steam explosion, and core concrete interaction. 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. The deluge lines connecting the GDCS pool to the lower drywell do not require the actuation of squib actuated valves on the GDCS injection lines to perform their functions. Temperature and pressure in the containment vessel are controlled by providing for a Passive Containment Cooling System. To assure availability, no valves are employed. More evidence should be provided on the functioning of the BiMAC, which has been developed to the conceptual level only. The use made of data bases and test programmes referred to should be reviewed in greater detail at the next step.

Uncertainties (statistic and deterministic) are included in the core layout, stability analysis, and scale-up considerations, etc. An in-depth review of their potential systematic deviation, propagation during the transients, and consequences on the results of the safety analysis for DBA and BDBA sequences should be performed.

The computer codes simulating the behaviour of the implemented novel features have mostly been derived from validated computer codes. This validation should be outlined in more detail including scaling considerations. The computer codes to be used for the melt-arrest device (BIMAC) and their validation are not yet developed. Codes simulating fuel behaviour for high burn-ups should be developed and validated. In this regard, the high burn-up behaviour under DBA transients is a relevant safety issue (code validation, methodology, criteria).

Generic site envelope

The documentation includes a list of the envelope site parameters for the ESBWR. If the site-specific parameters fall within the envelope, the site is considered suitable for locating the ESBWR.

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. These are well above the IAEA minimum of 0.10g peak ground acceleration for SSE. The ESBWR is designed to envelop the 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 site will be covered by these conditions. This follows the traditional practice in the siting of standard plants.

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.

The PSA based seismic margin assessment is expected to result in a margin of 1.67 over the SSE for the standard plant. This is aimed at demonstrating the capability of an ESBWR plant to withstand beyond design basis earthquakes.

The external natural and human induced hazards to be considered in the siting of the ESBWR are provided. For a chosen ESBWR site the process for evaluating hazards from nearby industrial and military facilities is described. Selection of design basis human-induced hazards is done using a probabilistic threshold of 1E-07/year.

Impacts from adjacent sites and malicious threats to the plant will be examined in detail during licensing for a particular plant site.

Based on the review of provided documentation it appears that the ESBWR design is in line with the applicable IAEA Fundamental Safety Principles. The review also indicates that the safety case is presented in a sufficient level of detail to allow assessment in most cases of whether the IAEA Requirements have been addressed. Several issues requiring further detailed review or more evidence and information were identified and are briefly addressed in the summary of review results above. These issues are discussed in greater detail in the individual review sheets provided in Attachment 4.

References

- [1] Nuclear Power Station Generic Design Assessment – Guidance to Requesting Parties, HSE, July 2007, Version 2
- [2] IAEA Safety Standards, Fundamental Safety Principles, Safety Fundamentals No. SF-1, International Atomic Energy Agency, Vienna 2006
- [3] IAEA Safety Standards Series, Safety of Nuclear Power Plants: Design, Requirements, No. NS-R-1, International Atomic Energy Agency, Vienna 2000
- [4] IAEA Safety Standards, Safety Assessment for Facilities and Activities, Draft Safety Requirement, DS348, International Atomic Energy Agency, Vienna 2006
- [5] Defence in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group, International Atomic Energy Agency, Vienna 1996
- [6] Assessment of Defence in Depth for Nuclear Power Plants, Safety Reports Series, No. 46, International Atomic Energy Agency, Vienna 2005
- [7] IAEA Safety Standard Series, Site Evaluation for Nuclear Installations, Safety Requirements, NS-R-3 International Atomic Energy Agency, Vienna 2003

ACRONYMS

| | |
|--------|---|
| AECL | Atomic Energy of Canada Limited |
| ALARA | As Low As Reasonably Achievable |
| ALARP | As Low As Reasonably Practicable |
| AOO | Anticipated Operational Occurrence |
| ASME | American Society of Mechanical Engineers |
| BDBA | Beyond Design Basis Accident |
| BIMAC | Basemat Internal Melt and Coolability Device |
| CANDU | Canada Deuterium Uranium |
| CASAT | Centre for Advanced Safety Assessment Tools |
| CCI | Core Concrete Interaction |
| CDF | Core Damage Frequency |
| CNSC | Canadian Nuclear Safety Commission |
| DBA | Design Basis Accident |
| DCD | Design Control Document |
| DGNSR | Directorate General for Nuclear Safety and Radioprotection (France) |
| ECCS | Emergency Core Cooling System |
| EPRI | Electric Power Research Institute (US) |
| EUR | European Utility Requirements |
| GDSC | Gravity-Driven Cooling System (ESBWR) |
| GDA | Generic Design Assessment |
| HPSI | High Pressure Safety Injection |
| HPIS | High-Pressure Injection System |
| HSE | Health and Safety Executive (UK) |
| I & C | Instrumentation and Control |
| INPO | Institute of Nuclear Power Operations (US) |
| INSAG | International Nuclear Safety Group (IAEA) |
| IRSN | Institute for Radiological Protection and Nuclear Safety (France) |
| IRWST | In-containment Refueling Water Storage Tank (EPR) |
| LBLOCA | Large Break Loss of Coolant Accident |
| LCDA | Limited Core Damage Accident |
| LOCA | Loss of Coolant Accident |
| LRF | Large Release Frequency |
| LWR | Light Water Reactor |
| MSIV | Main Steam Isolation Valve |
| NRC | Nuclear Regulatory Commission (US) |
| NSOA | Nuclear Safety Operational Analysis |

| | |
|---------|--|
| PIE | Postulated Initiating Event |
| PSA | Probabilistic Safety Assessment |
| RCPB | Reactor Coolant Pressure Boundary |
| RCPs | Reactor Coolant Pipes |
| RCS | Reactor Coolant System |
| RP | Requesting Party |
| RPV | Reactor Pressure Vessel |
| RRC-A | Risk Reduction Category A |
| RRC-B | Risk Reduction Category B |
| SAMDA | Severe Accident Management Design Alternatives |
| SAP | Safety Assessment Principle (UK) |
| SBLOCA | Small Break Loss of Coolant Accident |
| SCDA | Severe Core Damage Accidents |
| SG | Steam Generator |
| SLB | Steam Line Break |
| SSC | Systems, Structures and Components |
| SSE | Safe Shutdown Earthquake |
| TG | Technical Guidelines |
| URD | US Utility Requirements Document |
| WENRA | Western European Nuclear Regulators' Association |
| 2A LOCA | Double ended break of a reactor coolant system |
| 2A SLB | Double ended steam line break |