

**IAEA Generic Review for UK HSE of New Reactor Designs against  
IAEA Safety Standards  
ACR-1000**

# IAEA Generic Review for UK HSE of New Reactor Designs against IAEA Safety Standards ACR-1000

## 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 partly addressed. Considering the potential of a nuclear reactor for core degradation accidents with large radioactive releases, limited safety analyses at this stage have been performed. More detailed analyses are underway.

As described in the Technical Summary, the ACR-1000 is an evolutionary design retaining basic CANDU design features while incorporating enhanced safety features including passive features. At this stage limited results of the accident analyses are provided. The documents listed to support the Head Document are at various stages of completion.

The AECL Assessment Document ‘ACR-1000 Events’ provides a list of the categories of Design Basis Events to be analysed. Some selected ‘design assist analyses’ and analyses to support the PSA provide preliminary results or engineering judgements based on the details from the ACR 700 with updates for the ACR-1000. A number of more detailed analyses and ‘design assist analyses’ (meant to support and finalize the design) have been performed, including LOCA, pressure tube rupture, loss of regulation system, and main steam line break.

A series of very detailed documents claim compliance of the ACR-1000 design with the applicable UK HSE SAPs, the WENRA reactor safety reference levels and the Requirements contained in IAEA NS-R-1.

Both deterministic and probabilistic approaches are used to demonstrate that an adequate level of safety will be 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”. Special features are aimed at further slowing down or arresting severe core damage progression by providing a second passive core heat sink.

A detailed report has been prepared demonstrating that the ACR-1000 will comply with IAEA NS-R-1.

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

#### Review Results

The Requirement is addressed. The safety assessment makes reference to the maturity of the design. As described in the 'Technical Summary' the ACR-1000 is an evolutionary design retaining basic CANDU design features while incorporating enhanced safety features. A number of important analyses is available, but a significant part of the analyses is not available at this stage. However, the Head Document and the technical guidelines and reports state that the regulatory safety requirements will be met. A UK Requirements Compliance document has been prepared.

Further detailed safety assessments for the ACR-1000 will need to be supplied for the later steps in the GDA process. Important analyses such as pressure tube rupture were not part of the submission.

**3.5–3.6**

**3.5 At the start of the safety assessment, a judgement shall be made on the scope, extent, and level of detail and on 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, only a Preliminary Safety Report had been requested. The Requirements to be addressed are commensurate with the potential radiation risk arising from an NPP.

This Requirement is fulfilled if the Requirements specifically developed for NPPs as specified in NS-R-1 and national standards are followed. The report ACR Compliance Review with NS-R-1 indicates how the design complies with the Requirements of IAEA NS-R-1.

## 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

At this stage of the ACR-1000 design no information has been provided on the results of a safety assessment. Rather the information provided consists of a Head Document following the structure of the UK HSE request and several AECL documents. The Head Document provides information on how the design will meet the UK requirements and describes the process established for leading to a PSAR and a FSAR. The preliminary result of this process has been described in the UK requirements compliance document. The set of AECL documents contain the philosophy, requirements, safety design guides and methodologies to be used for the ACR-1000 design. A number of safety analyses (e.g. LOCA, PTR, steam line rupture, and 'loss of regulation' – control system) have been documented as well as some fault tree analyses for the development of the PSA. These documents address the IAEA Requirement.

The document 'Plant Performance Specification, Safety and Licensing Requirements for the Advanced CANDU Reactor' specifies that compliance with IAEA NS-R-1 is mandatory.

There will be two categories of DBAs based on frequency of occurrence and two categories of core damage accidents, Limited Core Damage Accidents and Severe Core Damage Accidents.

Two documents outline the methodology to be used for the Level 1 and 2 PSA. It is indicated that no Level 3 PSA will be performed. However, the Level 2 results will be 'interpreted' to address risk based safety criteria.

The Head Document makes reference to the limited design review of the ACR 700 by the USNRC and the pre-licensing review by the Canadian Regulator CNSC of the ACR-1000 which was not fully completed.

Only limited results of a safety assessment are available.

**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 documentation includes a safety design guide on radiation protection. It is indicated that internationally accepted limits and the ALARA principle will be adhered to. It is claimed that the ICRP60 limits will be met by a substantial factor, on the basis of previous CANDU experience. It is indicated that the analysis of severe accidents will identify cost-effective design mitigation at an early stage in the project.

No assessment results have yet been provided.

**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 ACR-1000 safety design guidance addresses the categories of this Requirement. Additional sub-categories for DBAs and core damage accidents will be introduced. It is planned to interpret the PSA level 2 results to address Level 3 based safety criteria as specified in the UK HSE SAPs.

No assessment information has been provided. The document 'Plant Performance Specification, Safety and Licensing Requirements for the Advanced CANDU Reactor' specifies that compliance with IAEA NS-R-1 is mandatory.

**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; however, limited information only is made available at this stage. As described in the 'Technical Summary', the ACR-1000 is an evolutionary design retaining basic CANDU design features while incorporating enhanced safety features. Passive safety features include Passive Emergency Coolant Injection, an elevated reserve water tank in the upper level of the containment and a large concrete reactor vault, surrounding the core in the calandria vessel and containing a large volume of light water to further slow down or arrest severe core damage progression by providing a second passive core heat sink.

At this stage, limited results of the accident analyses are provided to determine whether the design and engineered safety features fulfil the safety functions required of them. The documents listed to support the Head Document are currently at various stages of completion. The AECL Assessment Document 'ACR-1000 Events' provides a list of the categories of Design Basis Events to be analysed. The process for identifying ACR Events is depicted in Figure 2-2 of the Head Document. However, the document 'Systematic Review of Plant Design for Identification of Initiating Events' indicated to provide more details will be available at a later time only. A number of safety analyses and 'design assist analyses' is available, such as LOCA, PTR, steam line break and 'loss of regulation' (control system) as well as some fault tree analyses. Some selected 'design assist analyses' and analyses to support the PSA provide preliminary results or engineering judgements based on the details from the ACR 700 with updates for the ACR-1000 at this stage.

A series of very detailed documents claim compliance of the ACR-1000 design with the applicable UK HSE SAPs, the WENRA reactor safety reference levels and the Requirements contained in IAEA NS R-1\*.

Two categories of Beyond Design Basis Accidents (BDBAs) are addressed, namely, Limited Core Damage Accidents (LCDAs) and Severe Core Damage Accidents (SCDAs).

Preliminary results of PSA are provided in the documents 'Analysis Basis, and Probabilistic Safety Assessment (PSA) – Level 1 Methodology and Level 2 Methodology'. It is claimed that the project internal targets of 1.0E-6 for CDF and 1.0 E-7 for LERF are met, and thus the international safety goals and the UK HSE overall requirements\*. It is indicated that the Level-2 PSA will consist of an assessment of potential bounding containment scenarios. Cost/Benefit analysis will be used to demonstrate that no further risk reduction measures would be cost-effective.

---

\* Preliminary Review of ACR- 1000 Compliance with 2006 UK Safety Assessment Principles, Compliance Assessment of the ACR-1000 Against the WENRA Reactor Safety Reference Levels, ACR Compliance Review with NS-R-1

\* Note: UK HSE has no requirements on Core Damage Frequency

At this stage, preliminary results of accident analyses only are presented partly based on available updates from earlier designs, in particular the ACR 700. Based on these results the Requesting Party claims that the applicable requirements of the UK HSE, US NRC, WENRA, and IAEA will be met.

It is noted that the preliminary information of the document 'ACR-1000 Events', chapter 4.1.3, indicates that as a limiting case, following a LOCA, an earthquake of the Site Design Earthquake (SDE) level occurring 24 hours or more after the event is postulated and considered in the design basis conditions.

Since the PSA methodology including some preliminary results is provided only, the PSA should be reviewed in detail in the next step. It is noted that the PSA Level 2 will be a bounding containment scenario analysis.

Several safety features respond to the NS-R-1 Requirement to address in the design specified accidents beyond the design basis, including selected severe accidents.

**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. The documentation includes a safety design guide on radiation protection and documentation on how ALARA is achieved. It is indicated that the analysis of severe accidents is used to identify cost-effective design features aimed at accident prevention and mitigation. Various such design features are included in the design.

The assessment results are preliminary at this stage.

**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 4.19. Efforts to minimize radioactive waste are briefly described in the Head Document and in the Technical Description 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. Cost/Benefit analysis will be used to demonstrate that no further risk reduction measures would be cost-effective.

**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 Result

The Requirement is addressed through adherence to the Requirements and guidelines representing the defence-in-depth concept as described in the document ACR Compliance Review with NS-R-1. The design includes enhanced safety features, including passive safety features to address DBA and severe accidents, thus strengthening the 3<sup>rd</sup> and 4<sup>th</sup> level of defence-in-depth.

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

The basic safety approach to the safety of the ACR-1000 is deterministic. It is an evolutionary design making use to the extent possible of design features of operating CANDU reactors. The approach is complemented by probabilistic analyses.

It is noted that based on the CANDU design emphasis in defence-in-depth is given to the concept of multiple physical barriers.

**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; however, limited information only is available at this stage. A number of analyses have been done to demonstrate the safety under the accidents considered, such as LBLOCA, SBLOCA, PTR, Steam line break and loss of regulation. The preliminary deterministic analyses are complemented by preliminary probabilistic analyses. A PSA Level-1 and a bounding PSA Level-2 analysis will be prepared.

A document has been prepared that describes how the ACR-1000 design meets the WENRA reference levels. The document, however, is fairly narrative, in the sense that it describes the process how the WENRA levels are met, without giving much quantitative evidence. A similar approach has been followed for the UK requirements, where the compliance will be shown once the PSA is completed.

Based on the preliminary information available, it is claimed that the Requirements of IAEA NS-R-1, WENRA reference levels and UK HSE SAPs will be met.

The analysis of accidents beyond the design basis, including PSA, 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 Requirement is addressed in detail. Figure 2-5 of the Head Document gives a schematic of the primary computer codes used in ACR safety analyses. Details for the use of the codes are provided in the document 'Summary of ACR-1000 Computer Code V&V Process'. The document also referred to the related test facilities used in the process. In addition, a document has become available that explicitly describes the verification and validation process of the various computer codes used. For thermal hydraulic analysis, the CATHENA code is used. The PSA makes use of the CAFTA code. Additional information is provided in 4.60.

The use of the computer codes is well documented.

**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 document 'ACR-1000 Technical Summary' make extensive 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. A process of 'design assist analysis' has been followed to select the best option from a variety of possibilities for certain safety systems.

Chapter 8 of the document 'Review of the ACR-1000 against the UK requirements on ALARP' lists the improvements made in comparison to the CANDU 6.

The iterative process of the ACR design is well documented throughout the various documents demonstrating that the ACR-1000 is an evolutionary design.

## 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 partially addressed. The documentation claims that the ACR-1000 will fulfil the requirements of Canadian standards, which are equivalent to the IAEA Requirements. In addition, a separate document has been developed indicating compliance of ACR-1000 with IAEA NS-R-1.

The analysis basis for the ACR-1000 includes a presentation of the safety analysis approach for the ACR, including safety goals and acceptance criteria. A number of design basis analyses has been performed, which demonstrate that the applicable (technical) design criteria are met. Releases which are associated with the various events have not been determined. Some of the documentation is at an early stage of development.

In another document the radiation dose limits for the public are defined for normal operation (1 mSv/year) PPS Table 2-2, for AOOs (0.5 mSv) and DBAs (5 mSv) (Safety and Licensing Requirements for the ACR, PPS Table 2-4). These are the Safety and Licensing Requirements for the ACR and shall be met by the ACR-1000. In the document review against UK criteria, 10820-01000-ASD-001, sec. 6.2.2, it is stated that the release limits of the CANDU 6, which are below the UK criteria, can be applied.

In document 10820-01321-PPS001, Plant Performance Specification, chapter safety goals, section 2.2.2, Large Release Frequency (LRF), says: “the sum of frequencies of all event sequences that can lead to release to the environment of more than  $10^{15}$  Bq of Cs 137 shall be less than  $10^{-6}$  per plant year.” This statement is in disagreement with the safety target defined in Analysis Basis for ACR, document 108-03600-AB-003, which in section 3.5.2 states that: “the sum of frequencies of all event sequences that can lead to release to the environment of more than  $10^{14}$  Bq of Cs 137 shall be less than  $10^{-6}$  per plant year.”

In subsequent discussions with the HSE and from comments from AECL we have learned that since the issue date of the current version of the Plant Performance Specification (PPS), the CNSC issued a revised draft RD-337 with the requirement for LRF of  $10^{14}$  Bq of Cs-137. Therefore this will be corrected in the next revision of the Plant Performance Specification (PPS) report. This lower large release limit is already adopted as performance target by ACR as stated and correctly identified by the IAEA in the Analysis Basis for ACR. The Requesting Party has indicated that the lower limit will be met by the ACR-1000.

The ACR-1000 technical description states that PSA studies estimate that the summed frequency of internal initiating events leading to reactor core damage during at-power operation is only  $3.4 \times 10^{-7}$  for the ACR 700 and is expected to be better for the ACR-1000. This exceeds EPRI requirements by approximately two orders of magnitude and is comparable to the latest LWR designs. The assessment of implementation of this Requirement shall continue in the next stages of GDA review.

## 4.20–4.21 Safety functions

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

### Review Results

The guideline on safety classification identifies the three fundamental safety functions in line with NS-R-1. In addition, a fourth safety function (monitoring the status of releases to the environment) was introduced.

The safety functions are described in general terms [108-03650-SDG-001-NP Ch.3.2.1 and App.B, Tab. B-1 and B-2. A Secondary Control Area exists [10820-01010-PPS-001 Ch.6.1]. It is claimed that all generic Safety Principles and Criteria will be met [Head Document Ch. 2.4.2]. In the Technical Description, 10820-01371-TED-001, the safety functions are described in some detail. A number of analyses for design basis accidents has been submitted (LBLOCA, SBLOCA, PTR, steam line break, and loss of regulation) in various reports, and a preliminary list of all events to be analysed has been submitted (Table 1 in the Licensing Submission Scope Safety Analysis, 108-03500-LS-001). These other analyses have not been submitted at this stage.

The documentation reviewed is insufficient to assess fully the implementation of the Requirement in detail. However, because proven designs are used, it is possible that all the different sub-requirements will be addressed.

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

#### Review Results

This Requirement is addressed. Redundancies are implemented as well as the single failure criterion [108-03600-AB-003 Ch.4; 10820-01321-PPS-001 Ch.5.1]. Common Cause failures are addressed extensively [108-03660-AB-001-NP Ch.5.5; 108-03650-SDG-004-NP Ch.3.2]. The safety case package has been established to confirm the adequacy of the key mitigating design features [108-03660-AB-001-NP Ch.10]. The QA procedures are described in detail [164-01913-QAM-001-NP].

A detailed description of the safety functions is contained in the Technical Description 108200-01371-TED-001, which describes design elements such as protection against single failure, needed redundancy and physical separation, and environmental qualification. The assessment of the evidence that guarantees that all provisions are adequate should be part of the next step detailed safety assessment, which should include the review of the results of the PSA.

## **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 partially addressed.

(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 or accident conditions are generally addressed in Safety Design Guide Radiation Protection 108-03650-SDG. Site-specific assessment is proposed after a site is selected.

(b) The identification of natural and human induced hazards that have the potential to affect the plant is described in ACR 108-10100-PPS-001-NP (see Table 4 and Appendix E). 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 site-specific evaluation once a plant location is selected. ACR-1000 will be designed to an AECL standard ground motion spectrum anchored to 0.3g peak ground acceleration.

Airplane crash is mentioned in Section 2.2 of the Head Document as part of site selection. The modern international requirements on aircraft impact design are discussed.

c) The distribution of the population around the site and its characteristics with regard to any siting policy of the State and its neighbouring State is not discussed in the documents reviewed.

The general approach for treating the natural and human-made hazards follows the IAEA and other international standards. The specific assessment is expected following the site-selection.

**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.

A. The site assessment is very specific to the site selected. The procedures for selecting the site and identification and evaluation of hazards follow accepted industry practice and are in line with the IAEA Requirements for NPPs (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 do some limited design modification or conclude that the site is not suitable.

B. There is no discussion of periodic review of the site assessment in the Head Document; at the design stage of a new plant, this is not considered essential.

## **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 partially addressed. The documentation claims that the ACR-1000 reactor will provide adequate measures to protect people and the environment from the harmful effects of ionising radiation, but all results of safety assessments are available yet.

The Technical Description, 108200-01371-TED001, and a number of safety analyses indicate that provisions are designed as required by this Requirement. Radiological consequences of accidents are not yet analysed – it is claimed that the CANDU 6 results are a good estimate for the ACR1000, ref. Review against UK criteria, 10820-01000-ASD-001, sec. 6.2.2.

A full review will be undertaken when the safety analyses have been completed and the PSA has been submitted.

**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 partially addressed. The documentation claims that the ACR-1000 reactor will provide adequate measures to protect people and the environment from the harmful effects of ionising radiation within any relevant dose limits, but only a limited number of safety assessments are available.

Radiation protection is addressed in the Technical Description, 108200-01371-TED001. The ALARA concept has been addressed in the Review against UK criteria, 10820-01000-ASD-001. The documentation claims that: “The requirements from regulatory documents applicable to ACR-1000 will be considered with an appropriate level of implementations (i.e. mandatory or non-mandatory). They include regulatory policies (App. B to PPS), and regulatory requirements (App. C to PPS). Regulatory Standards describing rules, characteristics or practices which CNSC accepts as meeting the regulatory requirements are listed in App. D. to PPS.” Finally, the documentation says “In the fourth level of safety and licensing are the –ACR-1000 project requirements and guides which are developed with the intent to comply with the regulatory requirements described above. Their list is given in Table 3-1.”

Table 2 on Design Basis Internal Event contains titles of DBEs, but more information should be provided in the next stage.

An evaluation of whether protective measures are adequate is not possible at this stage.

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

**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 partially addressed.

There is a statement that the plant will satisfy the requirements of standards for normal operation, anticipated operational occurrences and accident conditions when the design of ACR-1000 has been completed. See further comments under paragraphs 4.24 and 4.25.

## 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. Plant Performance specification, section 6.4 states that proven technology shall be employed where practical throughout the plant, including system and component design, commissioning and start-up features, maintainability and operability features, and construction techniques. Documentation claims that the feedback from existing CANDU Plant Life Management (PLiM) and Plant Life Extension (PLEx) programs together with the large CANDU experience base of operating plants and construction projects shall be used to minimize the risk to the plant owner and constructor, and to simplify existing CANDU designs. Where enhanced technologies are incorporated into the design, demonstration through the ACR Research and Development (R&D) Program and/or proven successful use in other applicable industries will be required (6.4). The CANDU safety systems were critically reviewed for application to the ACR-1000 and improvements have been identified and applied, notably the addition of water injection systems to improve the natural circulation (thermosyphoning) capability of the HTS.

Operational experience including results of root cause analysis of anticipated operational occurrences and accidents has been reflected in Generic Action Items (GAIs) developed by the CNSC. PPS part Safety and Licensing Requirements for the ACR-1000 states that the ACR-1000 design will provide design solutions to the GAIs. Direct design solutions shall be implemented, and for issues where direct design solutions are not feasible, AECL will ensure that the major contributors to nuclear safety risk and the major sources of uncertainty associated with the issue have been identified and addressed. The list of CNSC GAIs is given in App. A to PPS.

Detailed assessment of implementation of this Requirement needs to be undertaken in the next stages of GDA review.

**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 partially addressed. The ACR-1000 Technical Description formulates design principles observed in the design.

The ACR-1000 submission for Step 2 of UK GDA, Part 1 HSE NII requirements, section 2.4.4 states that “the review of the ACR-1000 safety principles and criteria against the requirements for the UK is expected to demonstrate that all fundamental safety principles and criteria are fully reflected in the ACR-1000 Safety and Licensing requirements documents.” Further evidence to support the achievability of the Safety principles and Criteria is provided in section 2.5, and 2.6.

The documents ‘Compliance Assessment with the NS-R-1’, ‘Compliance Assessment against UK SAP’ and ‘Compliance Assessment against WENRA requirements’ all claim to show that the compliance is assured.

The document states that “all past CANDU plants have met their safety principles and criteria as they have been licensed and are operating safely around the world”. The analysis results for the ACR 700 design, which is a precursor of the ACR-1000, also showed that the applied safety principles criteria and requirements have been achieved. Therefore, this provides confidence that the ACR-1000 will also achieve its safety principles criteria and requirements.”

The PPS Plant Design Philosophy describes in a general way the licensing requirements to the plan and safety requirements to safety equipment. The principles which should assure plant resistance to design basis accidents, core damage prevention and accident mitigation are formulated in general way (section 5.1.4).

Several requirements described in the documentation of ACR-1000 are typical for modern nuclear power plants, such as:

- Redundancy in safety equipment and clear procedures “single failure criterion”
- Fail safe operation where practical separation and independence form each other and from process systems, to the extent practical, with a limited sharing of sensors between process and some Safety Systems
- High reliability of system actuation on demand
- Seismic qualification
- Environmental qualification
- Protection against impact and dynamic loads

Although various documents describe the implementation of these principles, the next step safety assessment should address these issues in detail.

The requirements for DBAs, core damage prevention and accident mitigation provide some insights into the safety level to be assured by the plant systems. In particular, the following issues should be clarified in the next stage:

1. For core damage prevention one of the additional requirements states that “The ability of each unit to withstand loss of offsite AC power and one set of onsite diesels for at least 24 hours without fuel damage shall be provided (5.1.2)”. It should be clarified whether in case of LOOP and loss of one set of diesels the remaining diesels can still assure safe shutdown in long term.

2. Accident mitigation measures included robust containment, with the design pressure based on the limiting design basis event.

2a. The pressure in case of a severe accident should be clarified. Modern international good practice includes designing containment so that it would not fail even in case of a severe accident. More information is needed on the capacity of containment to withstand a severe accident.

2b. A hydrogen control system is present, so that H<sub>2</sub> concentration for DBEs and LCDAs does not exceed limits commensurate with the probability and severity of the event. It should be clarified whether this means that deflagration to detonation transition is excluded or can be accommodated. Statement related to limits “commensurate with the probability and severity of the event” and possible containment failure due to hydrogen burning should be clarified.

2c. Thickened pre-stressed concrete structure designed to withstand aircraft crashes (ACR-1000 Technical description, section 1.3). The kind of aircraft crash that the ACR-1000 containment can withstand should be specified.

The documents listed to support the Head Document *are* complete and adequate to address NII’s GDA Step 2 requirements, i.e. provide the claims for nuclear safety of ACR-1000 design, including the requirement for a suitable documented safety assessment. More information is already available but was not provided to NII as the scope for Step 2 GDA was to assess the claims. The arguments and evidence to support the claims, in this case the detailed ACR-1000 safety analyses will be provided as per NII’s GDA Steps 3 & 4 requirements in the PCSR to be submitted in Steps 3 & 4.

Some information can be made available only to NII (as it would be of protect-commercial nature) while some only to OCNS as it would contain security sensitive information. One example of the latter is information that would answer reviewer’s question on aircraft impact design.

Further discussion of defence in depth is provided under article 4.45.

The next step safety report should clarify these points and provide more detailed and clear information on the safety level of the plant.

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

#### Review Results

The Requirement is partially addressed. It is the intention of the designers to ensure that all novel elements will be tested, but only high level description of testing programme is available at present.

The definition of novel elements is provided in section 2.2 of the Licensing Submission. For those novel elements technology gap reports were prepared and reviewed. The results of these activities were incorporated into the ACR-1000 research and development program during the detailed program planning process. The list of novel elements is provided in Part 1 HSE NII requirements, section 2.12.3. They include:

- Containment steel liner on the inside surface of reactor building, planned to be installed instead of epoxy lining as in the past CANDU;
- Modifications to the reactor assembly;
- Replacement of both the liquid zone control and guaranteed shutdown liquid poison provisions with a rod-base system;
- Use of light water in the heat transport system;
- Change in header and feeder material, Upgrades to the fuel handling and storage system; and
- Upgrade to the control system.

Also some improvements of the ECI have been proposed, e.g. a ‘keep full’ system to enhance the natural circulation (thermosyphoning) capability in the case of SBLOCA.

These novel features are included in the detailed scope of the ACR-1000 Design Verification Plan (DVP). DVPs are developed and describe design and testing verification activities to be performed for each phase of the project. The scope of the R/D program is defined in general terms in section 3.3 of Licensing submission.

According to the statement in 2.12.3 “this ensures that the ACR-1000 structures, systems components and engineering tools including novel features, will perform in accordance with their safety and operational requirements”.

More specific information should be included in the next step safety report.

**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

This Requirement is addressed. The classification of structures, systems and components is described; it is based on a risk approach consistent with frequencies and consequences [108-03650-SDG-001-NP Ch. 3]. A list of codes and standards used for the design of structures, systems and component has been provided (document 108-03650-DG-004).

Initiating events and their classification using PRA results are described [108-03600-AB-003 Ch. 3.2; 10820-03600-ASD-001 Ch. 3]; acceptance criteria are given [108-03600-AB-003 Ch. 3.3]. Its importance for safety is considered; probabilistic considerations and frequencies are used to group events [108-03600-AB-003 Ch. 3.2].

Licensing requirements and safety design guides are presented [10820-01321-PPS-001-NP Ch. 3 and App. D and E]. It is stated that the design of the ACR-1000 will be compliant with the applicable National Standards of Canada for CANDU plants [10820-01321-PPS-001-NP Ch. 4 and App. F].

The next step safety assessment should address whether sufficient classification is also established from the defence-in-depth point of view, and whether it is comparable to international experience (e.g. classification standard ANS 58.14). Items that warrant attention are:

- classification for pressure integrity, i.e. the closer a component is to the active fuel, the higher its classification; also sufficient redundancy should be provided in isolation devices from the primary system (now sometimes one isolation valve is provided where two are common practice);
- classification of items that are not directly relevant for mitigation of releases, but where fission product boundaries/defence-in-depth is involved (e.g. a steam line break requires the containment spray to protect containment integrity, but as the event would not lead to releases the spray is considered non-nuclear safety); similarly, non-LOCA events and external events need capability to protect the primary system integrity, to shut down the reactor and maintain it in a safe shutdown state; the systems providing these functions should all be safety-grade;
- classification of items that are not formally safety, but can prevent actuation of safety systems (e.g. the reactor regulation system is capable of preventing safety system actuation, but is considered non-safety) – these need no formal classification, but should

be subject to additional oversight, inspections, testing, etc. In some other regulatory frames these are called ‘supplemental safety’;

- classification of items that mitigate BDBA, LCDA and SCDA; these are now non-safety (class D), but should be subject to additional design and operational requirements, possible also classified as ‘supplemental safety’, as discussed above. For some of the accidents, full classification inside DBA should be considered, e.g. for primary feed and bleed assuming all secondary heat removal is unavailable.

It should be established that for the ‘weight’ of the mitigative features, one should select an appropriate conservative fission product source. For example, to classify systems that mitigate SGTR, radioactive contamination of the primary system should be assumed, even where the leakage of CANDU-fuel is very low. For systems that mitigate transients (e.g. steam line break), leakage to the secondary side should be assumed, from a contaminated primary system, as discussed above.

Details, e.g. results for frequencies, consequences, radiation doses, etc. should be required.

**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

This Requirement is generally addressed although many specific details are not included in the documents provided by AECL. ACR 10820-03600-ASD-001 lists the external hazards to be assessed. The generic site envelope is described in the Plant Performance Specification Site Characteristics ACR 108-10100-PPS-001. If the site-specific external events fall within this generic site envelope, then that site is deemed appropriate for locating an ACR-1000.

In the PSA for external events (108-03660-AB-001-NP), a PSA-based Seismic Margin Assessment is proposed. It is aimed 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 too severe for the UK sites.

At the time of the review, design against aircraft impact was not found in the documents reviewed and should be part of the next step safety assessment. Also the impact of Electro Magnetic Pulse (EMP) is not discussed. Note: in a number of nuclear reactors in Western countries such protection is implemented in the design.

**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

This Requirement is addressed. Tables 4 and 5 of 108-03600-ASD-001 list the internal hazards to be considered in the safety assessment. The internal hazards include fires, explosions, pipe breaks, internal floods and turbine missiles. The philosophy behind combining different internal and external hazards is described in this document. Details are, however, missing.

The next step safety assessment should address all aspects of internal hazards (i.e., pipe whip forces, jet impingement forces, internal flooding and spraying, load drop, missiles from rotating machinery and valve stems) in the detailed design following the AECL and IAEA standards and international good practices.

**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 partially addressed. ACR-1000 design for the RCS follows the Canadian N-standards (Vol. 1, sec. 2.8.3), which are similar to the corresponding ANS-standards. Hence, selection and application of materials are in conformance with appropriate standards. The applicable CSAs have not been studied by reviewers, but it is anticipated that they provide a similar approach as the ANS-standards. Also reference is made to the ASME-code. Hence, it is anticipated that due attention is paid to the behaviour of material under transient and accident conditions.

No detailed technical information was found, hence the presence of typical characteristics such as leak-before-break behaviour (LBB) is unknown. No efforts have been found that the number of welds is reduced, or that there are no seam welds in the headers. It is unclear whether moulded parts are used in the RCS-piping, or that all has been forged or wrought. Sec. 6.4 of the PPS refers to the use of proven technology – there is no reference to specific techniques developed since.

The conclusion is that the mechanical design and the material selection follow established codes and standards but may not go beyond that (e.g., LBB).

On the basis of the studied material, it cannot be concluded that the mechanical/material aspects are addressed in a complete and comprehensive way.

The ACR-1000 fuel is based on the CANFLEX fuel, used in earlier designs. A research and development program is in place for the verification of the fuel design for the ACR1000 (Compliance with NS-R1 document, 10820-01321 ASD002 NP, sec. 3.2.3.2). The next step safety assessment should assess the outcome of this program, notably to assess whether the fuel will meet the conditions for the intended higher burnup, compared to earlier CANDU designs.

No information was found on aspects such as fuel swelling, pellet clad mechanical interaction (PCMI), chemical effects and maximum fuel centre line temperature. The conclusion is that the documentation is insufficient to assess the aspect of fuel and associated (i.e. cladding, control rods) materials. This should be part of the next step safety assessment.

The RCS design should be further assessed with respect to number of welds, sort material (preference no moulding), reduction of irradiation of material, LBB-behaviour.

**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 reviewed documentation shows that the Requirement is partially addressed by reference to the IAEA NS-R-1 Safety of NPP-Design. According to Part 1 HSE NII requirements , section 2.8, the mandatory codes and standards include IAEA NS-R-1 Safety of NPP-Design, and according to that document, fail safe design should be applied where possible. It is probable that similar requirements are included in the Canadian codes and standards, which are also mandatory for ACR-1000.

Similar statements are provided in Safety and Licensing requirements for ACR, section 3.3.1, which says “compliance with NS-R-1 is mandatory from the ACR project perspective and, in addition, ACR-1000 intends to consider other Requirements of the IAEA to the extent practicable. ...The ACR-1000 project shall identify the applicable IAEA documents that the project will apply.” (3.3.1).

The Technical Description, doc. 10820-01371-TED-001, describes in a number of items the application of the fail-safe principle. The next step safety assessment should address the issue in more detail.

**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 ACR-1000 design for the RCS follows the Canadian N-standards (Vol. 1, sec. 2.8.3), which, according to AECL, are similar to the corresponding ANS-standards. Hence, selection and application of materials are in conformance with internationally accepted and widely used standards (the applicable CSAs have not been studied by reviewers). Also reference is made to the ASME-code. Hence, it is anticipated that due attention is paid to the behaviour of material under transient and accident conditions, which includes consideration of fatigue.

From the documents studied, notably the Technical Description, doc. 10820-01371-TED-001, it appears that no generally applied in-service inspection regime like ASME XI is applied, adapted to the specifics of the ACR-1000 design. The next step safety assessment should address this issue in detail.

Ageing is considered in the CNSC Generic Action Items (GAI) 90G03 in Table A1 of PPS001, which is called 'Assurance of Continued Nuclear Safety - Management of Aging', and is completed (i.e. closed). It is a subject of the Plant Reliability Approach (PPS001, sec. 3.3) and part of the Plant Life Management System (PLiM), which is discussed in the PSA documentation, 108 - 03360 AB01 NP, rev. 2, page 6-2. The PLiM provides systematic assessment, timely detection and mitigation of significant ageing in critical systems, as identified in the PSA.

Ageing is discussed in the qualification for harsh environment, in Safety Design Guide SDG03, sec. 3.1.5, including the ageing stressors (factors that cause ageing, such as temperature, radiation, pressure, humidity, etc.). The documents submitted do not discuss how the requirements/recommendations of SDG03 have been implemented.

The conclusion is that the designer has considered the time related effects in a complete and comprehensive way. However, the documents studied do not provide much detail on the envisaged in-service inspection methodology, neither on the actual implementation of the ageing management.

1. Arts. 4.33 and 4.35 are closely interlinked. The consideration of material aspects (4.33) includes the consideration of time effects (4.35).
2. A further assessment should be made as to whether the PLiM covers the time-related effects of all relevant components over the full plant life. The assessment should include the methodology of in-service inspection.
3. The acceptability of the usage factor should be considered, as often the limited value is restricted to 0,5 but some designs allow 1,0. In the latter case, appropriate safety margins should be in place.

**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 partially addressed. PPS Plant Design Philosophy section 4.2 speaks about the necessity of environmental qualification, and similarly as in 4.34, the Requirement is addressed in an indirect way, namely by reference to the IAEA NS-R-1 Safety of NPP-Design. According to Part 1 HSE NII requirements, section 2.8, the mandatory codes and standards include IAEA NS-R-1 Safety of NPP-Design, and according to that document, equipment qualification is required. Similar requirements are included in the Canadian codes and standards, which are also mandatory for ACR-1000.

At the time of the review no direct statement concerning the level of equipment qualification could be found. The next step safety report should provide information on equipment qualification for ACR-1000.

**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 submission addresses the Requirement for decommissioning provisions.

The submission details the design characteristic incorporated into the ACR to facilitate decommissioning (108UK-01600-700-002 Rev 0 - Para. 2.5). These include:

- Civil/Architectural design features;
- Radiological & non-radiological zoning design;
- Open top construction & reactor building components;
- Reactor building and storage bay liners; and
- Fuel design & handling

The submission also highlights the need to maintain integrity of the buildings during the expected 60yr operating life and an additional 32 years to cover possible Storage with Surveillance Period.

Decommissioning objectives and possible strategies are specified 108UK-01600-700-002 Rev 0 - Para. 3). The reference strategy discussed is a combination of prompt and deferred decommissioning options - demolition of the Balance of Plant immediately after safe sustainable shutdown and subsequent isolation and storage of the nuclear portion of the plan for a pre-determined time.

## **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 submission documentation partially addresses the Requirement. However, it includes only general statements regarding human factors engineering or human system interfaces. No specific information could be identified regarding the procedures that will be developed to operate the plant during normal, abnormal conditions or severe accident management.

The Plant Design Philosophy document details the Plant Safety Approach (3.2) and includes a general comment on applying Human Factors Engineering principles and criteria in the design of systems, facilities, equipment and procedures. A similar general comment is made regarding Plant Operability (3.3.1).

Also the Plant Design Philosophy document comments that Human Factors (6.5) will be systematically taken into consideration in the design of systems, facilities, equipment and procedures. Human Factors Guidelines and a Human Factors Engineering Program Plan are referenced (Ref 12). However, at the time of the review there was no document identified in the reference section under reference 12.

Human factors in the design have been described in the Technical Description, doc. 10820-01371-TED-001, in various places. The item, hence, has received extensive attention.

The results of PSA should be used in developing the operating procedures. The next step safety assessment should address the human factor and human system interfaces issues in more detail. It should be also assessed whether there is a statement on procedure development and support by the Requesting Party.

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

Review Results

All submitted documents have been reviewed. However, no relevant information addressing the Requirement could be identified.

No reference could be found in the submitted documentation regarding the suggested staffing requirements, their necessary qualifications and experience and staffing levels.

It has been stated in the Technical Description, doc. 10820-01371-TED-001, that staff can be reduced about 10% compared to equivalent size CANDU 6.

It should also be noted that there is a general trend to reduce staff in nuclear power plants in many countries. Hence, the next step safety assessment should consider this matter in detail.

The submitted material does not address the IAEA Requirement.

.

**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 submission documentation partially addresses the Requirement. However, it includes only general statements regarding human factors engineering or human system interfaces. No specific information could be identified regarding the guidance in the development of procedures.

The Plant Design Philosophy document details the Plant Safety Approach (3.2) and includes a general comment on applying Human Factors Engineering principles and criteria in the design of systems, facilities, equipment and procedures. A similar general comment is made regarding Plant Operability (3.3.1)

Also the Plant Design Philosophy document comments that Human Factors (6.5) will be systematically taken into consideration in the design of systems, facilities, equipment and procedures. Human Factors Guidelines and Human Factors Engineering Program Plan are referenced (Ref 12). However, at the time of the review no document identified in the reference section under reference 12 was available.

With regard to Operability (7.1.1) a state of the art Control Room will be designed; systems and controls to minimize Control Room Operator Error will be developed and actions related to abnormal operations will be practical to perform and validated during the design phase. See further discussion to art. 4.38.

In the next stages of the GDA reviews the Human Factor and Human System Interfaces issues need to be addressed in more detail. A statement should also be requested on Procedure development and support by the Requesting Party.

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

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

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

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

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

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

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

**4.48** The safety assessment 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 Defence-in-depth (DiD) is explicitly addressed in the Plant Performance Specification (PPS), sec. 3.2. In addition, the ACR-1000 is on the one hand a well-proven design, which is based on an evolution of a series of CANDUs over many years, which complied with the DiD concept, and on the other hand an advanced design that is set up to strengthen the various safety functions. For example, a major improvement over earlier designs is that the ACR-1000 has a negative reactivity power and void feedback coefficient under nominal power conditions (note: further assessment should establish whether the coefficient is also negative during credible off-normal conditions).

In addition, the ACR-1000 has been submitted for review by the USNRC and this body declared to expect that the ACR-1000 would meet its rules and regulations, which would include fulfilment of the DiD-concept.

The review team did not assess all features which would confirm the application of the DiD, but believes, on the basis of the foregoing arguments, that the design addresses the DiD concept. Further elements confirming the application of DiD are described below.

Plant PSA is used to demonstrate that accident frequency analysis meets applicable regulatory criteria. Note: further assessment is needed to establish whether the PSA has also been used *to improve the design*. Such feedback would strengthen the DiD-concept on most or all levels. This should be a subject of the next step safety assessment.

Plant design is such that it can be adapted to meet various regulatory standards, such as IAEA (PPS, sec. 4.1) -which would mean a.o. an obligation to meet the DiD-concept.

The ACR-1000 specifies also another suitable design philosophy to meet the DiD, by approaching plant safety in three subsequent levels: accident resistance, prevention of core damage and accident mitigation (PPS, sec. 5.1).

In levels 2 and 3, the ACR-1000 provides both active and passive safety features. Active systems have the advantage that operating experience is available.

In level 4, systems and equipment credited for mitigation of BDBAs (in ACR-1000 terminology: LCDAs, Limited Core Damage Accidents) will be assessed for this purpose, but without formal classification. This assessment strengthens the DiD level 4, but the actual benefit can only be acquired by further insights in the process. Reviewers have preference for a defined, dedicated classification. This should be a subject of the next step safety assessment.

A further benefit in level 4 is that the ACR-1000 provides various features to mitigate severe accidents (PPS, sec. 5.1.4), including a passive moderator and shield water cooling, and to assess instruments for behaviour under severe accidents.

In level 4, DiD, the review team notes AECL's statement that, apart from the avoidance of short-term containment failures, also long-term over-pressurisation of the containment will not occur (Safety Basis, sec. 3.4). The team did not assess the value of the underlying arguments, which should be the subject of the next step safety assessment.

The ACR-1000 design includes provisions designed for the development of severe accident management guidelines (SAMG) - PPS, sec. 5.1.4. Note: reviewers did not assess whether these actually have been developed or are under development for the ACR-1000. The present state of the art for CANDU SAMG is that such guidance recently was developed and is under implementation at CANDU-plants (2007). A useful feature of the SAMG execution is a

Technical Support Centre., which is available in the ACR-1000 (ref. Technical Description, doc. 10820-01371-TED-001, sec. 7.6.1)

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), other than that there is an emergence Secondary Control Area (PPS, sec. 6.1, Technical Description, sec. 7.6.1.1).

DiD-issues to be covered in further in-depth assessments:

Functionality of the connection to the grid, for robustness in level 2, DiD. The ACR-1000 is designed for switching from full power to house load, but it should be further assessed whether it has a sufficiently robust connection to the grid (e.g., two independent lines) and is capable of load rejection at 100% power. Basic statements on these issues are presented in the Technical Description, doc. 10820-01371-TED-001, sec. 8.

Role of normal control systems to reduce the number of actuations of safety systems (level 2, DiD).

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.

Passive systems have limited driving forces and, hence, are sensitive to line blockage or sticking check valves, as incidents in the past have shown. Operation of these systems should be shown to be effective by adequate margins in a detailed assessment, and it should be substantiated that the lessons from past incidents have been learned.

Most of the technical basis for severe accident mitigation has been developed for LWRs and not for CANDU. Transition from the LWR- insights to the ACR1000 should be done with great care and assessed accordingly in a further in-depth assessment. An example of such transition is the development of the MAAP4-CANDU code.

Protection against hydrogen combustion is offered for DBA and LCDA (PPS, sec.5.1.3). It should be assessed to what level also full core damage accidents are covered, i.e. those that melt the calandria and initiate basemat attack.

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 ACR1000-design, but it was not possible within the limited time available to see whether the issues are covered to full depth.
- sec. 4.48: safety margins are addressed in the ACR-1000 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.

The ACR-1000 concept is based in part on passive safety systems. Although passive systems offer advantages, there is also a risk that the driving forces are too small to overcome blockages and sticking check valves.

The DiD concept in the ACR-1000 should be further analyzed, 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 solid basis in the present-day understanding of severe accidents, also because the insights have been developed mainly for other reactor types.

## **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 partially addressed, since limited information only is available at this stage. The AECL documents 'Safety Basis for ACR' and 'ACR-1000 Events' consider, consistent with NS-G-1.2, a list of postulate initiating events including release of radioactive material from a subsystem or component and shut-down state. The 8 categories of PIE are grouped into AOOs 2 categories of DBAs and two categories of BDBAs. However, it is indicated that the document 'Systematic Review of Plant Design for Identification of Initiating Events' will be available at a later stage only.

Regarding the post-operational state, a Design Guide 'Design Features Facilitating Decommissioning' is summarizing the features aimed at reducing "dismantling time, radiation source and the volume of radiation waste". In addition, there is a document titled 'Overall Decommissioning Strategy for CANDU Reactors', 108UK 01600 700 002.

A series of very detailed documents claim compliance of the ACR-1000 design with the applicable UK HSE SAPs, the WENRA reactor safety levels and the Requirements contained in NS-R-1. Reference is made to the limited design review of the ACR-700 by the US NRC and the precicensing review of the ACR-1000 by the Canadian Regulator CNSC, which was not fully completed. The documentation also makes reference to the experience in licensing CANDUs in foreign countries.

Based on the documents guiding the design it is claimed that the Requirements will be met.

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

#### Review Results

The Requirement is addressed. The document 'Review of the ACR-1000 against the UK Requirements on ALARP' provides data from past experience. It is argued that the dose to the public from normal operation will be less than 0.01 mSv/year. The total staff exposure target is less than an average of 1 person-Sv/year. Based on past experience it is claimed that the criteria of the UK HSE SAPS for AOOs and DBAs will be met. At this stage the analyses for AOOs and DBAs have not yet been finalised, and only selected 'design assist analyses' and analyses to support the PSA are available only. Some analyses have been provided, e.g. LBLOCA, SBLOCA, PTR, steam line rupture, loss of regulation. Radiological consequences have not been described, but it is stated that these are comparable to CANDU 6. In addition, a number of events will be analysed, as described under art. 4.26.

The DBA analysis will include as a limiting case, following a LOCA, an earthquake of the Site Design Earthquake level occurring 24 hours or more after the event.

In addition to the design basis accidents, the accident analyses will include, consistent with NS-R-1, specified accidents beyond the design basis, including severe accidents.

Preliminary results of PSA are provided in the documents Analysis Basis, Probabilistic Safety Assessment (PSA) – Level 1 Methodology and Level-2 Methodology. It is claimed that the project internal targets of  $1.0E-6$  for CDF and  $1.0 E-7$  for LERF are met, and thus the international safety goals and the UK HSE requirements. It is indicated that the Level-2 PSA will consist of an assessment of potential bounding containment scenarios. Cost/Benefit analysis will be used to demonstrate that no further risk reduction measures would be cost-effective.

The document 'Safety Basis for ACR (Dec 2006)' specifies acceptance criteria and performance targets for 'Limited Core Damage Accidents' (LCDA) and 'Severe Core Damage Accidents' (SCDA). In case of LCDAs the calandria will stay intact.

The probabilistic performance targets are given as follows: The total frequency of accidents leading to 'small releases' from LCDAs should be less than  $1.0 E-5$  per plant year, based on 'design-centred assumptions'. The frequency of SCDA should be less than  $1.0 E-5$  per plant year. The frequency of releases to the environment from SCDA of more than  $1.0 E+14$  Bq of Cs-137 shall be less than  $1.0 E-6$  per plant year, based on realistic and best-estimate assumptions.

However, the document 'Safety and Licensing Requirements for the Advanced CANDU Reactor ACR-1000 (Feb 2007)' specifies a small release as less than  $1.0 E+15$  Bq of I-131, but a large release as  $1.0 E+15$  Bq of Cs-137.

Regarding releases the documents also use different definitions of what constitutes a 'plant'.

Preliminary results of accident analyses only are presented, partly based on available updates from earlier designs, in particular the ACR-700. Based on these results it is claimed that the applicable requirements of the UK HSE, US NRC, WENRA and IAEA are met. Not enough information was found on the functioning of the advanced safety features.

**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. The AECL documents 'Safety Basis for ACR' and 'ACR-1000 Events' consider a list of postulated initiating events including releases of radioactive material from a subsystem or component. In accordance with the frequency of occurrence they are grouped into AOOs, two categories of DBAs, and two categories of BDBAs. The document 'Systematic Review of Plant Design for Identification of Initiating Events' will be available at a later stage only. See further the discussion in Requirement 4.26.

Detailed results of safety analyses, including the performance enhanced safety features are only available for a number of events. Radiological consequences are estimated on the basis of the CANDU 6 results (ref. art. 4.26).

Some inconsistencies were found in the definition of targets for severe accidents, as described in 4.50.

At this stage of the ACR-1000 design, very limited information on the results of safety analyses is available.

---

<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 ACR-1000 design follows the Safety Design Guides (PPS001, sec. 3.2), which identify safety-related systems, and provide guidance how to address the Requirements for applicable code classifications, seismic qualification, environmental qualification, separation of systems and components, fire protection, containment and radiation protection. In parallel, PSA has to be conducted to assure that accident frequency analysis will meet regulatory acceptance criteria, and to demonstrate that quantitative safety goals are met.

Consequently, it is intended that both deterministic and probabilistic approaches are in place. Relevant documents include the following: Assessment Document -10820-01321-ASD-004-NP, Revision 0 (1 Head Document); Safety Basis - ACR-1000 108-03600-AB-003-NP, Revision 1; Events, ACR-1000 10820-03600-ASD-001-NP, Revision 0; Probabilistic Safety Assessment (PSA) – Level 1 Methodology-108-03660-AB-001-NP, Revision 2; Probabilistic Safety Assessment (PSA) – Level 2 Methodology- 108-03670-AB-001-NP, Revision 0. The documents outline methodologies to be followed and contain some of placeholders for future information.

On the basis of the above documentation, no conclusion could be reached on the actual implementation of an integrated decision making process. This should be part of the next step safety assessment, 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

PPS001, sec. 2.6.2 specifies safety analyses as follows:

- Conservative deterministic analyses (Limit of Operating Envelope)
- best estimate uncertainty analysis
- design-centered / best estimate deterministic analyses

The first two bullets are to demonstrate that all AOOs and DBAs are within prescribed limits. The last bullet is to demonstrate adequate control of BDBA up to and including severe plant conditions.

In order to define appropriate design rules and requirements, SSC should be classified according to their safety role, with design requirements commensurate with the safety function. Such classification is performed according to 108-03650-SDG-001. This document is in line with (and refers to) IAEA NS-R-1. Some further comments and some cautions regarding classification are expressed under art. 4.30. 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. The selected design rules and the margins obtained should be further studied, to confirm the safety margins which the applicant claims. At present, safety class D is assigned, which specifies commercial grade for the equipment in that class, i.e. it is non-safety.

The USNRC declared that it expects the ACR-1000 to meet its rules and regulations. Also from this perspective, a proper safety classification is expected to be in place. The above regulations do not specify detailed design rules and requirements for equipment to mitigate BDBAs up to and including severe accidents. Consequently, the intention of the Requirement of 4.54 is addressed for a large class of safety-related SSC. Detailed safety assessment should confirm whether these analyses actually are in place and are acceptable for all safety-related SSC.

For the analysis of some events, as presented in the LBLOCA analysis and the 'design assist analysis' of the ECI and LTC, a number of comments and cautions can be expressed:

1. The nodalization selected appeared to be a one-dimensional type of flow: an average channel simulated a whole quadrant of channels (~ 130). It should be further assessed how the hottest channel will behave. The use (if any) of hot channel factors and peaking factors should also be further assessed.
2. For a geometry with many parallel channels, it cannot be assumed that they will not influence each other. Various instability mechanisms exist, e.g. the Ledinegg instability (two different mass flows can exist for the same pressure difference between inlet and outlet headers), and the parallel channel instability (channels behave like a mass and

spring system between a given pressure difference). It should be assessed to what extent such mechanisms can influence the cooling capability. Notably because under oscillations, the critical heat flux (CHF) can be lower.

3. The criteria provided seem to be sufficient to demonstrate the efficiency of the ECI /LTC. The technical basis for these criteria should be assessed. The so-called 'international' peak clad temperature (PCT) criterion of 1200 EC has a technical basis from the LWR. It should be assessed whether this criterion is also valid for the ACR1000. In addition, the other LWR-criteria specify a maximum allowed oxidation (17%) and a maximum H<sub>2</sub> -generation (1%). It should be assessed what the equivalent criteria are for the ACR1000 or, in other words, why these criteria are not also used.
4. The maximum clad temperatures are fairly high (up to 1180 EC). Yet, no uncertainty analysis has been provided, or even discussed. A limited number of sensitivity analyses have been performed, but these - of course - do not replace uncertainty analyses.
5. Both flow increase as flow reversal are seen as mechanism to improve cooling, versus the stagnation that is calculated to occur at specific break sizes. It should be further assessed whether in flow reversal, at the moment of stagnation, no CHF will be exceeded. In principle, such calculations require a dynamic CHF-correlation (e.g. used by GE for their BWRs. In the verification / validation document, it is mentioned that for the ACR1000 CHF-correlation has been developed(10820-01321 Computer Code Validation ASD-012). The documents do not contain technical detail to assess the statements re the CHF-correlation, which should be in the next step safety assessment.
6. For the cases with loss of external grid (LOOP), the generator trip and subsequent loss of power have been assumed at the moment of turbine trip. It should be assessed what is the consequence of simultaneous LOOP, as is the international practice for the LWR. Note that keeping pumps running may remove a large amount of heat, which otherwise will drive up the fuel temperature (but see also item 8).
7. The cases analysed depend on the availability of the secondary loop to remove decay heat. It should be analysed what the plant capabilities are without this circuit (i.e., primary feed and bleed).
8. A typical measure in LWR-ECCS is to trip the RCPs upon the occurrence of LOCA, in order to decrease the mass loss from the RCS (running pumps will make the coolant to two-phase liquid, which has a high mass loss at the break, whereas idle pumps may lead to only steam mass loss, after the initial two-phase mass loss, with a much lower mass loss). It should be investigated what the equivalent action at the ACR1000 would be and what its benefit might be.
9. As some of the transients can place considerable loads on mechanical components (e.g. the crash cool down places a large transient on the primary system and parts of the steam generators (notably the tube sheet)), the next step safety assessment should address structural integrity of mechanical components. It should also be addressed what will happen with components that are not or not timely isolated from the primary system (e.g. the pressuriser), if such isolation failure is credible or should be postulated.

**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 not addressed in the documentation reviewed. A PSA for the ACR-1000 was not yet available and was not required by the HSE for the Step 2 GDA. (This Requirement is complemented by further Requirements of NS-R-1, in particular the Requirement 5.37).

Chapter 2.6 of the submission documents refers to the UK requirements for PSA. This chapter refers to the documents '108-03660-AB-001, Revision 2, July 2006' and '108-03670-AB-001, Revision 0, January 2006', which describe the Level 1 and 2 PSA methodologies to be used in the assessment. These documents constitute a procedure for conducting the probabilistic safety assessment, containing considerably detailed information on how different parts of the safety analysis are conducted with some particularizations for CANDU designs. In addition to the processes, methods and techniques to develop a Level 1 and 2 PSA, the documents refer only to the probabilistic safety targets that the design will meet, but without any evidence or indication of having actually conducted an analysis to prove it and to identify the significant contributors to the risk of this design.

Since Level 3 PSA is neither a requirement nor a common practice in Canada, the intention for the UK licensing submissions to interpret the Level 2 PSA to address the Level 3 (risk) based safety criteria is specified in the SAPs.

In addition to this, the documentation includes separate probabilistic analyses of the following safety systems: Emergency Feedwater (EFW) system, Reserve Water System (RWS), and Moderator system. According to 2.6.13 of the submission document, the Essential Cooling Water/ Essential Service Water (ECW/ESW) and Plant Cooling Water/ Plant Service Water (PCW/PSW), was also analysed. These analyses are reliability analysis of the safety system functions of limited scope, e.g. failure of support systems is not considered, using common fault tree analysis techniques.

It can be concluded that only a reliability assessment of a few individual safety systems has been conducted, which does not address the goals and analysis approaches stated in 4.55. The next steps of the GDA process shall focus on the review of the expected detailed PSA documentation.

Documents 108-03660-AB-001 and 108-03670-AB-001 are only procedures for conducting a level 1 and 2 PSA for a NPP with particular considerations for CANDU designs. No analysis has been conducted.

Probabilistic safety analyses of some safety systems have been conducted using the fault tree analysis technique. The analyses consider only intrinsic failures, i.e. failures of support systems are not considered. The analyses used the ACR1000 reliability data base for component failure probabilities and consider human errors and common cause failures (Beta factor method). Quantifications are carried out with the code CAFTA. All tables, with data, analysis information and results are left blank in the documentation. Therefore, limited insights can be gained at this point on the adequacy of these analyses.

## 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 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: At this stage of the ACR-1000 design limited information has been provided consisting of a Head Document following the structure of the UK HSE request and a set of AECL documents at various stages of completion. For some of the reports listed it is stated that they will be published later. The set of AECL documents contain the technical summary description, design philosophy, requirements, safety design guides and methodologies used for the ACR-1000 design. At a later stage, various other documents have been provided, which include a.o. a technical description, and a number of safety analyses for DBA.

The Head Document and the document ACR-1000 Technical Summary describe the development of the ACR-1000 as a long-term evolutionary process making use of the experience gained from the CANDU-9 and CANDU 6 designs. The Technical Description provides details of the design. 'Design assist analysis' is performed to optimize some emergency systems.

The basic safety approach to the safety of the ACR-1000 is deterministic. The approach is complemented by probabilistic analyses. At this stage preliminary results of accident analyses only are presented partly based on available updates from earlier designs. Based on these results it is claimed that the applicable requirements of the UK HSE, US NRC, WENRA, and IAEA will be met. The process established for leading to a PSAR and a FSAR is described.

The document 'ACR Compliance Review with NS-R-1' provides a detailed paragraph by paragraph review of the ACR-1000 design against the NS-R-1 document. It is claimed that the applicable Requirements are met. Another document provides a 'Compliance Assessment of the ACR-1000 against the WENRA Reactor Safety Reference Levels'.

A PSA for the ACR-1000 is not yet available. Two documents outline the methodology to be used for the Level 1 and 2 PSA. It is indicated that the Level 2 PSA will be based on potential bounding containment scenarios. No Level 3 PSA will be performed. However, the Level 2 results will be 'interpreted' to address Level 3 based safety criteria as specified in the UK HSE SAPs. Preliminary results of PSA are provided in the documents 'Analysis Basis,

Probabilistic Safety Assessment (PSA) – Level 1 Methodology and Level-2 Methodology'. It is claimed that the project internal targets of  $1.0E-6$  for CDF and  $1.0 E-7$  for LERF will be met, and thus the international safety goals and the UK HSE requirements.

The document 'Safety Basis for ACR (Dec 2006)' specifies acceptance criteria and performance targets for 'Limited Core Damage Accidents' (LCDA) and 'Severe Core Damage Accidents' (SCDA). In case of LCDAs the Calandria will stay intact.

The document 'ACR-1000 Events', chapter 4.1.3, indicates that as a limiting case, following a LOCA, an earthquake of the Site Design Earthquake (SDE) level occurring 24 hours or more after the event is postulated and considered in the design basis conditions.

The Head Document makes reference to the limited design review of the ACR 700 by the USNRC and the pre-licensing review by the Canadian Regulator CNSC of the ACR-1000 which was not fully completed.

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 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.

Two documents specifically address the UK HSE SAPs. The document 'Review of the ACR-1000 against the UK requirements on ALARP' provides some preliminary information mainly based on an extrapolation of results from the CANDU 6 Safety Report for normal operation and design basis accidents. However, the corresponding Tables 6 and 8 to be included for demonstrating compliance were not included in the document reviewed.

The document 'Preliminary Review of ACR-1000 Compliance with 2006 UK Safety Assessment Principles' provides a compliance statement for each of the UK HSE SAPs stating how they will be met by the design. Regarding the SAP NT.1, the following is stated: "The limits and targets adopted by the reference ACR-1000 design are those included in Canadian nuclear legislations and regulatory documents. For projects outside Canada, verifications are performed to ensure that the limits and targets applicable to the host country are met." No results are given on how the numerical targets included in NT.1 will be met.

Detailed information is provided on the criteria used by the designer based on Canadian requirements and the SAPs of the UK HSE. It is noted that there are differences which relate in particular to criteria for fault sequence analyses and the use of PSA that are identified and will be addressed in further analyses.

At this stage only preliminary results of accident analyses are presented, partly based on available updates from earlier designs. Based on these results it is claimed that the applicable requirements of the UK HSE, US NRC, WENRA and IAEA will be met. In particular, no detailed information was available on the functioning of the advanced safety features.

There seem to be some inconsistencies in the definition of significant releases between different design documents and differences in the probabilistic targets between these documents and the PSA guidelines, as described under 4.50.

A PSA for the ACR-1000 is not yet available. The PSA methodology guidance including some preliminary results is provided only. Therefore, the PSA shall be reviewed in detail in the next steps of GDA. It is noted that the PSA Level 2 will be a bounding containment scenario analysis. There are no plans to perform a Level 3 PSA. However it is planned to interpret the Level 2 results on how Level 3 criteria will be 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

These Requirements are considered in the reviewed documentation.

Substantial margin is claimed to be included in the ACR-1000 design to address the level of uncertainties associated with the current validation base. In the case of the physics codes, initial validation exercises serve to confirm the applicability of the physics tools within the large margins. Current validation work in progress is used to reduce the uncertainties [10820-01321-ASD-002-NP and 10820-01321-ASD-012-NP].

To complement the validation performed using data from test facilities, AECL is benchmarking its physics codes against the Monte Carlo physics code MCNP and against a third party suite of physics codes that are not being used for the core design analysis or the safety analysis. The results of the benchmarking activities completed to date confirm that the uncertainties arising from calculations with the ACR physics codes are within the safety margins set for the ACR design.

The data used in the design and safety analysis are either existing valid data or data based on specific experimental results. Large scale test facilities are in use - partially adapted – to validate the thermal-hydraulic codes.

---

<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.

One of the normal practices in analysis is that conservative assumptions are made in design or related safety analyses (e.g. a power level of 102 %, a maximum temperature of 1100 °C during LOCA, etc.) to cover any uncertainties. Extrapolation from available data is avoided, or will be done with appropriate justification.

Deterministic safety analysis is performed for Anticipated Operational Occurrences and Design Basis Accidents. When traditional limit of operating envelope analyses for design basis events do not indicate significant margins, an alternative is to use the best estimate and uncertainty method (BEAU). However, in the analyses that have been submitted (LBLOCA, SBLOCA, PTR, loss of regulation, steam line break), no uncertainty analysis has been presented, although some of the calculated values are quite close to the criteria (e.g. 1180 °C where the limit is 1200 °C). A number of sensitivity analyses have been performed in the ECI and LCT 'design assist analysis', but these do not replace uncertainty analysis.

As part of the development of the PSA, uncertainty analyses are performed on parameters such as failure rates, component unavailabilities, initiating events, and human error probabilities. The uncertainties for each of these quantities are expressed in terms of probability distribution about their mean or best-estimate values. Sensitivity analyses are performed to test the impact of certain changes in key input values.

Uncertainty elements are classified as natural randomness of a quantity and as lack of knowledge of a quantity. The latter is divided into model uncertainty, parameter uncertainty and completeness uncertainty. The first two have been reduced by significant improvement in knowledge as a result of knowledge from international R&D programs and collaboration. Completeness uncertainty can be reduced by independent peer review processes.

The next step safety assessment should include the validation of the codes used, and the uncertainty analysis for relevant parameters.

Data for uncertainties and results of sensitivity studies should be presented.

For AECL it is important to develop a methodology document to ensure that the design includes sufficient margins to cater with process parameter variations, process parameter uncertainties measurements, analysis uncertainties and maintenance activities.

## 4.60 Use of computer codes

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

### Review Results

The Requirement is addressed. The ACR-1000 design is an evolution from the proven CANDU 6 designs in terms of the overall reactor configuration, including safety systems and safety-related system configuration and functions. This results in the fact that event sequences and physical phenomena associated with postulated accidents in an ACR-1000 are common, for most part, with those events in a conventional CANDU reactor. Therefore, only a few computer codes and experimental data base extensions consistent with the different operating conditions of the ACR-1000 (mainly higher pressure, higher temperature, higher enrichment, and use of light water coolant) require modifications.

Details of the validation work are presented in the document Computer Code Validation, 10820-01321-ASD-012.

For the analysis of the physics the codes WIMS, RFSP and DRAGON are used. Data for validation are from the ZED-2 zero power lattice test facility.

The CATHENA computer code is the primary tool for transient thermal-hydraulic system behaviour. This code has been extensively validated at various test facilities, notably the large scale RD14-M facility and the Cold Water Injection Facility (CWIF). The RD14-M facility is being modified so that it includes all the features of the ACR-1000.

The ELESTRES code models the fuel behaviour under operating conditions while the ELOCA code models the fuel behaviour under accident transient conditions. The codes have been adjusted to the higher enrichment in the ACR-1000 fuel; their validation uses data from fuel element tests in the NRU reactor and data for higher burnups from operating CANDU reactors.

The GOTHIC-IST code is use for containment thermal-hydraulics and hydrogen behaviour. Fission product behaviour in the containment is simulated with SOPHAEROS and SMART-IST. MAAP CANDU is used for severe core damage during severe accidents.

It is claimed that substantial margins are included in the design to address the level of uncertainties associated with the current validation base.

An extensive AECL software quality assurance program is outlined. [ACR-1000 : 10820-01321-ASD-012 Rev.0].

It should be shown that the fuel code is capable of modelling high burnup fuel also for transient conditions. The burnup will be around 20000 MWd/ton, which is not really high burn-up from the LWR perspective (values go up to 70000 MWd/ton), but is substantially above present day CANDU burnup.

## 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 5.10**

**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 submission addresses the use of Operating Experience Feedback into the design process. However, no specific information could be found in the submission regarding actions taken or lessons learned from significant international Operating Experience, especially from other reactor designs.

It states in the Head Document, Section 2.2.3, that AECL has implemented a Feedback Monitoring System (FMS) which captures OEF and ensures that the issues are addressed in future designs. This is based on Canadian National Standards (N283.2.00 Section 3.4). In addition, the Radiation Protection aspects of the design include an ALARA programme.

Feedback of operating experience through FMS will be based on Canadian standard N286.2-00 (Licensing Submission document, sec. 3.4), but this is an activity of the designer (AECL), not of the licensee, and it is unclear if and to what extent this information is made available to ACR-1000 licensees.

The submission does not mention the need for the utility to establish a data collection system that can be used to update the safety assessment throughout the operating life of the plant

Appendix F of the Head Document details various novel features and their importance to safety – several of these quote operating experience as one of the initiators of the development of the features, for instance:

- Guaranteed Shutdown achieved by rod-based systems rather than liquid poison
- Fuel Handling System improved and simplified following operating experience.

Quality Assurance Manual section 4.6 states that Feedback information and lessons learned from previous designs, procurement, manufacturing, construction, installation, commissioning, licensing and operations are received, reviewed, assessed and fed back into the designers to be incorporated into the design in accordance with applicable procedures.

The Technical Description refers to the use of operating experience in the matter of radiation protection, of existing CANDU stations. International operating experience feedback is not considered.

Neither data collection nor reference to safety performance indicators, as addressed in Requirement 4.61, was not found in the documents submitted. Therefore, 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 (Req. 4.35).

As the Requirement 4.61 is written for an operating nuclear facility, it could be considered as not applicable at the design stage. However, it is recommended that the next step safety assessment addresses the issue.

## 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 not addressed. There is no safety report available at this stage. However, the documents provided indicate the intention of the designers to address this Requirement.

The documentation provided by ACR-1000 designers typically refers to Canadian standards, which include requirements consistent with the IAEA guidance and claims that so far all CANDUs have been fulfilling the requirements of standards, so it is expected that ACR-1000 will also fulfil them. However, this is not a sufficient basis to say that “the findings of safety assessment are documented”. Also, no results of assessment or analyses that have been carried out are available.

The Head Document (ACR-1000 Submission for step 2 of UK Generic Design Assessment, Part I H\*SE\_NII Requirements) states that the information on generic design should provide sufficient information on the design concept and principles, together with sufficient description of the design to provide the regulator with an understanding of the ACR-1000 design...and facilitate to identify the main nuclear safety hazard and the associated control measures and protection systems (2.1.2). However, more information is needed for an evaluation of this Requirement.

The assessment of the safety analysis results has not been made yet. The statement in section 2.4.4 says that “the review of the ACR-1000 safety principles and criteria against the requirements for the UK is expected to demonstrate that all fundamental safety principles and criteria are fully reflected in the ACR-1000 Safety and Licensing requirements documents”.

The reviews of compliance of ACR-1000 with UK SAPs (2.14.3) and with WENRA reference levels (2.14.4) were presented in addition to the previously submitted materials on 17 September 2007. They contain many positive statements of qualitative character, which indicate the intention of the designers to address all Requirements.

In the next stage of the work the safety report for ACR-1000 should be submitted.

The available documents display many blank spaces and material provided does not correspond to the Requirements of the IAEA. At this stage it is not possible to assess to what degree the IAEA Requirements have been addressed.

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

Review results

The requirement is not addressed at this stage.

No quantitative and qualitative outcomes of the safety assessment are given. There is no supporting evidence for and reasoning about the robustness and reliability of the safety assessment and its assumptions. What is provided, are the expressions of intentions of the Requesting Party stating that:

“all past CANDU plants have met their safety principles and criteria as they have been licensed and are operating safely around the world. The analysis results for ACR 700 design, which is a precursor of the ACR-1000 also showed that the applied safety principles criteria and requirements have been achieved. Therefore this provides confidence that the ACR-1000 will also achieve its safety principles criteria and requirements”.

Concerning information on the performance of individual system components there is a list of novel elements in ACR-1000 (2.12.3), which include:

- Containment steel liner on the inside surface of reactor building, planned to be installed instead of epoxy lining as in the past CANDU;
- Use of low enriched uranium fuel;
- Modifications to the reactor assembly;
- Replacement of both the liquid zone control and guaranteed shutdown liquid poison provisions with a rod-base system;
- Use of light water in the heat transport system; and,
- Change in header and feeder material, upgrades to the fuel handling and storage system, upgrade to the control system

These novel features are included in the detailed scope of the ACR-1000 Design Verification Plan (DVP). DVPs are developed and describe design and testing verification activities to be performed for each phase of the project. According to the statement in 2.12.3 “this ensures that the ACR-10000 structures, systems components and engineering tools including novel features, will perform in accordance with their safety and operational requirements”. However, full documentation should be submitted for assessment.

The Requirement should be reviewed at the next stage when the safety report and the safety assessment for ACR-1000 have been submitted for review.

**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 only partially addressed as some information pertaining to the safety case was provided but the SHR was not part of the submission.

**4.65 The safety report shall be updated as necessary. This safety report shall be retained until the facility has been fully decommissioned or the activity has been terminated. For a repository for radioactive waste, the safety report shall be retained for an extended period after it has been closed.**

#### Review Results

The Requirement will be addressed in any new NPP built in the UK.

The Requirement of updating the safety report within Periodic Safety Review PSR has been introduced in all EU countries and a NPP built in the UK will be obliged to satisfy this Requirement. The retention of a safety report and in fact all safety related documentation is also required and checked in practice, and it will be observed in the case of the new UK NPP, even if the documentation includes no explicit statement to that effect.