Health and Safety Executive

IAEA Generic Review for UK HSE of New Reactor Designs against IAEA Safety Standards
AP1000

IAEA Generic Review for UK HSE of New Reactor Designs against IAEA Safety Standards
AP1000

3.1–3.7 Graded Approach

3.2–3.3

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

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

Review Results

The Requirement is addressed. The scope, extent, level of detail and effort is consistent with the potential of a nuclear reactor for core degradation accidents with large radioactive releases. Following the standard DCD format of the US NRC a safety analysis has been performed to determine whether the design and engineered safety features fulfil the safety functions required of them. Detailed information is provided on how the safety objectives and criteria established by the US NRC, the UK HSE, and WENRA are addressed. The design makes use of the past experience with reactor operation and addresses the US and European utility requirements.

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

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

The possibility of occurrence of very low probability events with potentially high consequences is taken into account. In particular, design features are included, which respond to the IAEA NS-R-1 Requirement that “in addition to the design basis, the performance of the plant in specific accidents beyond the design basis, including selected severe accidents, shall also be addressed in the design”. Special features are aimed at arresting a molten core within the RPV by cooling the outside surface, thus avoiding challenges to the containment.

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

Review Results

The Requirement is addressed. The safety assessment makes reference to the maturity of the design by documenting the use of the extensive past operating experience for improving the safety of the plant. DCD Chapter 1.9 systematically addresses compliance with US NRC Regulatory Criteria including 'Three Mile Island Issues' and the list of 'Unresolved Safety Issues and Generic Issues'.

Results of safety assessments are presented for the innovative features. Reference is made to the verification of the assessments by experimental results. DCD subchapter 19.39 provides a summary of the severe accident phenomena. The extensive separate PSA report contains more detailed calculations. Increasing simplification and use of passive safety systems led to a reduction in the complexity of the design as summarized in Chapter A.2 of the Head Document on AP1000 Safety Philosophy. The safety assessment effort is reduced by the fact that support systems are not needed for fulfilling certain safety functions. However, increasing attention is given to the performance of passive features.

The DCD document subchapter 19.39 and the separate PSA document contain many references to documentation of experimental results from test facilities. This information could not be reviewed at this stage. Also the scaling of results for the AP 600 to the AP1000 has to be analysed in detail at the next step.

3.5–3.6

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

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

Review Results

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

4.1–4.15 Overall Requirements

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

Review Results

The Requirement is addressed. Detailed reference is made to the safety objectives and criteria established by the US NRC, the UK HSE, and WENRA. In addition information is presented on how the utility requirements in the US and in Europe are addressed. Both deterministic and probabilistic analyses are used to demonstrate that an adequate level of safety has been achieved. Section A of Document 1, the 'UK Safety Case Overview', provides summary information and guidance on where results of specific analyses have been reported in the DCD report.

The DCD report and the PRA provide safety assessment information using the standard format requested by the US NRC. Appendix C of Document 1 gives extensive information on how the analyses described in the DCD and the PRA for demonstrating compliance with the NRC criteria address the Safety Assessment Principles (SAPs) of the UK HSE.

Section B of Document 1 summarizes information on how the design addresses the US Advanced Light Water Reactor Utility Requirements (URD) and the European Utility Requirements (EUR). It is stated that the US detailed requirements for passive designs were developed concurrently with the AP 600 design. The most significant non-compliance areas with the EUR are identified, in the submission, as aircraft crash protection, fuel cycle length/MOX design and nuclear island layout. It is stated by the designer that there are plans for these to be addressed in the next step.

The AP1000 has undergone the US NRC design certification process. The NRC Final Safety Evaluation Report for AP1000 Design is appended as Section F of the documentation. It is stated that there are no open items.

The report addresses radiation protection requirements for workers and the public for normal operation and accident conditions.

Section D provides a road map cross-referencing the WENRA reactor safety reference levels with sections of the DCD. It is noted that the report claims compliance also in a case where it is stated that the "AP-1000 design uses an alternative approach". In this regard (Issue F 1.1 'design extension') the alternative approach is described in the Appendix 1 B of the DCD, Severe Accident Mitigation Design Alternatives (SAMDA). It should be noted that this issue of the WENRA safety reference level is consistent with the IAEA Safety Requirement to address "selected accident conditions beyond the design basis

accidents”. The IAEA Safety Standards do not include requirements consistent with the SAMDA assessment.

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

Review Results

The Requirement is addressed. Information is provided on how the radiological risks are being controlled within the limits specified by the SAPs of the UK HSE, which also reflect the IAEA BSS. A specific Section B of Document 1 addresses the application of the ALARP principle for the AP1000 design. The ALARP analysis provided in the documentation includes use of design experience, operational experience, industry standards, regulatory requirements and review, peer review and the USNRC SAMDA evaluation.

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

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

Review Results

The Requirement is addressed. This safety assessment Requirement is complemented by the more detailed principle technical Requirements in Chapter 4 and by the Requirements for plant design as provided for by NS-R-1. Information on how these requirements have been addressed is provided in Chapter 15 of the DCD. However, the analysis follows the standard US NRC procedure based on classification of plant conditions into the categories I to IV. Also, for calculating radiological consequences the standard NRC procedure is followed. In order to address these differences from the categories of the IAEA standards and the SAPs, Appendix C, the SAP road map for AP1000 design, provides information on how the events treated in plant conditions I to IV relate to the categories of fault sequences contained in the SAPs of the UK HSE.

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

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

Review Results

The Requirement is addressed. The design is based on the US Advanced Light Water Reactor Utility Requirements Document (URD). This document was developed in a formal process in the late 1980s/early 1990s to collect operating experience within the US. In addition to requirements for evolutionary designs, it also provides detailed requirements for passive designs. It is stated that these requirements were developed concurrently with the AP 600 design. In particular the passive safety systems and features include a passive core cooling system, passive containment cooling system, main control room emergency habitability system and improved containment isolation. No containment penetrations are required since the passive residual heat removal and safety injection features are located entirely inside the containment. DCD Chapter 1.9 systematically addresses compliance with US NRC Regulatory Criteria, including 'Three Mile Island Issues' and the list of 'Unresolved Safety Issues and Generic Issues'.

DCD Chapter 15 gives a list of the initiating events studied by category of plant condition I to IV. Subchapter 15.0.11 provides summaries of the principle computer codes used. The codes used in each transient are listed in Table 15.0-2. The Chapter then presents detailed results of the accident analyses to determine whether the design and engineered safety features fulfil the safety functions required of them. The analyses include events associated with potential radioactive release from auxiliary systems. The accident analyses include an assessment of the radiological consequences in accordance with US NRC requirements. As a conservative approach to containment performance major core degradation and melting is assumed, though the analyses show that core integrity is maintained.

Severe accidents with core degradation and melting are addressed by providing for flooding of the reactor cavity with IRWST water. This engineered safety feature is aimed at retaining the molten core debris in the RPV through outside cooling of the external surface. DCD subchapter 19.39 provides a summary of the severe accident phenomena. This approach addresses the NS R-1 Requirement to address in the design specified accidents beyond the design basis, including selected severe accidents.

Results of calculations and experiments are contained in the separate PSA report included in the documentation.

The Level 1, 2, 3 PSA including external events and shutdown risk has been performed. It has been used to optimize the design and to demonstrate compliance with the US NRC safety goals.

Many of the analyses including the PSA, have originally been performed for the AP 600. The documentation provides information in DCD subchapter 19.34 and PSA Chapter 34 on how these results have been extrapolated to the AP1000 design. This includes references to publications and reports which were not available within the framework of this review.

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

Review Results

The Requirement is partially addressed. Individual and societal radiation risks are calculated in accordance with the US NRC procedures for normal operation and accident conditions for workers and the public. They are further detailed in Section B of Document 1. Appendix C of Document 1 provides information on how the analyses described in the DCD and the PRA for demonstrating compliance with the NRC criteria address the SAPs of the UK HSE. The calculations of individual radiation risk follow standard US NRC procedures.

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

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

Review Results

The Requirement is partially addressed. A more detailed evaluation of the radiation risks posed by the facility is given under 4.19. Efforts to minimize radioactive waste are briefly described in DCD Chapter 20. Novel design features have been added to the design with the aim of significantly reducing the probability of severe accidents with potential long-term impacts. SAMDA assessments are presented to demonstrate that the ALARA principle has also been applied to severe accidents.

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

Review Results

The Requirement is addressed. The combination of several layers of protection is present throughout the design. However, the concept itself as summarized in subchapter A.2 'AP1000 Safety Philosophy' does not exactly correspond to the 5 levels of defence-in-depth as outlined in NS R-1. The design includes innovative features, in particular passive safety features designed to function without active safety support systems, such as AC power, component cooling water, service water, and HVAC.

The basic safety approach to the safety of the AP1000 is deterministic based on the defence-in-depth concept. The approach is complemented by probabilistic analyses of a Level 1, 2, 3, PSA including shutdown and external hazards.

A more detailed assessment of defence in depth is provided under 4.45 to 4.48.

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

Review Results

The Requirement is addressed. The safety assessment includes the results of safety analysis for events grouped into the plant conditions I to IV. The documentation in DCD Chapter 15 includes a description of the results of the safety analyses performed for the different initiating events. Details in form of diagrams of the thermal hydraulic analyses are provided. The basic approach to the safety assessment is deterministic following US NRC procedures. Special attention is given to describing the conservatisms in the analyses.

The deterministic analyses are complemented by a Level 1, 2, 3 PSA including risks from shutdown states and external events.

The analysis of accidents beyond the design basis makes 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. The DCD chapters 15 and 19 provide information on the computer codes used for the accident analyses and for obtaining the success criteria for the PSA. Chapter 34 of the PSA addresses the severe accident phenomena and refers to computer codes used and to a long list of reports and publications. More details are provided under 4.60.

The extrapolation of results from the AP 600 to the AP1000 should get special attention at the next step of the review.

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. Section B of the Head Document summarizes the development process of the US URD concurrently with the design of the AP 600. The design was also strongly influenced by the results of various PSA studies. Attachment B.3 lists the changes made to the AP 600 and the AP1000 design based on PSA. In addition, DCD Appendix 1.B provides a list of Severe Accident Mitigation Design Alternatives which, however, were not included based on SAMDA evaluations. A complete list of the standards used in the design is given in Table B.2 of the Head Document.

The iterative process of the AP1000 design is documented.

4.19 Potential Radiation Risks

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

Review Results

The Requirement is addressed. Radiation source strengths and specific activities are determined for the reactor core, for primary coolant (N-16 activity), fission and activation products, pressurizer liquid and gas phase, typical out of core crud deposits, chemical and volume control system components, spent fuel pool system components, liquid radwastesystem components, spent demineralizer resin, and residual heat removal system (Tables 12.2.1-12).

Spent fuel gamma source terms are defined, and calculated for control rods and other elements followed by determination of the molten core accident source term in containment is determined (Table 12.2-20).

Parameters and assumptions used for calculating containment airborne radioactivity concentrations are defined (Table 12.2-22) and the results given for a wide range of conditions (for no purge, with normal purge and with shutdown purge for 24 hours) (Table 12.2-23). Similarly the airborne radioactivity is determined for fuel handling area (Table 12.2-25) and/or auxiliary building (Table 12.2-26, 27).

Fission-product source terms are presented in Chapter 45, divided into intact containment IC, containment bypass BP, failure of containment isolation CI, containment failure induced by severe accident phenomena that may occur during the core melting and relocation phase of the accident sequence CFE, and containment failure that may occur after 24 hours CFL. The results in Table 45-1 and 45-2 show that the highest releases occur in the case of containment bypass and, since their contribution is also the largest, BP sequences are clearly the dominating hazard. However, their overall frequency is shown to be very low.

A comprehensive radiological analysis has been produced including off-site doses as shown in Chapter 46. The estimated site boundary whole-body dose and the acute red bone marrow dose are compared to the Westinghouse goal of <25 rems (0.25 Sv), at a frequency not to exceed 1 E-6/reactor-year.

In case of BP scenario, fission products are released from the reactor coolant system to the environment via the secondary system or other interfacing system bypass. Since containment failure occurs prior to onset of core damage, there is no time delay in fission product releases and no retention, so this scenario corresponds to the IAEA Requirement 4.19 to determine “potential radiation risks taking no credit for any safety features”. For the release categories – BP, CI, CFE, and CFI – the mean dose at the site boundary in 24 hours is greater than 25 rem. The sum of the probabilities of the release categories, including an intact containment excess leakage category, is approximately 2.4 E-7 events

per year for at-power conditions, so there is a large margin in the probability for meeting the Westinghouse design goal of the LRF to be less than 1 E-6/reactor-year.

In Table 49-3, dealing with doses at the exclusion area boundary, the highest dose is due to the scenario of containment bypass, which is logical, since in such a case there are no safety systems involved. This explains why the designers have taken pains to reduce as much as possible the hazard of containment bypass. There is a misprint in the number showing the peak consequence dose for BP sequence in Table 49-3 (last column). It is printed an order of magnitude too low. This should be corrected to 4.72E+02.

The core damage frequency for power operation (2.41E-07) is two orders of magnitude smaller than the corresponding values typically calculated for current PWRs.

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 Requirement is addressed. The safety functions are described in the executive summary, in section A and F as well as in the DCD. The safety functions provided by the principal fluid system are the control of reactivity, the RCS inventory and integrity, and the residual heat removal.

Special attention is paid to the passive core cooling system which provides the safety functions of core residual heat removal, safety injection and depressurization [Head Doc. Ch. A.1.2.5.1]. It is claimed that the related safety analyses, which are supposed to use approved computer codes, intend to demonstrate the effectiveness of the passive core cooling system in protecting the core, following reactor coolant system break events, up to a full double-ended rupture of a reactor coolant system main loop pipe.

The safety function ‘Control of Reactivity’ is addressed [DCD Ch.4.3.1.5]. This safety function covers operational occurrences up to accidents. The shutdown margins are such that the reactor can be made sub-critical from all design stages and maintained sub-critical. Adequate protection over the entire range of possible reactivity insertion rates exist [DCD Ch.15.4 and 15.4.2.3]. A Remote Shutdown workstation is available [DCD Ch.7.4].
The safety function ‘Heat Removal from the Core’ is carried out by passive systems – no AC power is needed. Active human action is required only after 72 hrs [Head Doc. Ch. A.1.1; DCD A 1.1].

The safety function ‘Confinement of Radioactive Materials and Control of Operational Discharges, as well as Limitation of Accidental Releases’ is addressed and the release values are well below required limits [Head Doc. A.3.4.6, DCD Ch.12.4.1.7 and Ch.15.7.4.5] for internal events as well as for external hazards.

Based on the three fundamental safety functions, the plant specific safety functions have been derived and are listed comprehensively in Ch 3.1. This is the basis for the identification and classification of the SSCs which follows the 10 CFR 50, ANS-58.14, ANS 51.1, Reg. Guide 1.26 and 1.97 and 10 CFR 21. All classified systems and related classification requirements are set out in dedicated tables (Table 3.2.1, 3.2.2, and 3.2.3).

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. Selection of proven components has been emphasised to ensure a high degree of reliability with a low maintenance requirement. The single failure criterion is applied [DCD Vol. 2 Ch.3.1; DCD Vol. 2 Ch.15.0.12]. Common Cause failures are taken into account [DCD Vol. 2 Ch. 19.59.3.2 and Ch.19.59.5.1] and its importance, especially for shutdown states, is shown [DCD Vol. 2 Ch. 19.59.5.1] although it should be recognized that the overall core damage frequency is very low. The AP1000 uses passive safety systems; its reliability is high resulting in core damage frequencies and large release frequencies well below the INSAG targets referred to in the IAEA Safety Standards [DCD Ch. 19 Tab. 19.59-17]. As mentioned previously for 4.20, the identification of the SSCs is associated with the corresponding requirements that explicitly consider the different types of failure as well as their consequences for safety. Info on single failure and common mode failures was not provided in the classification Chapter 3.2. A QA program applicable to the design, procurement, fabrication, inspection, and/or testing of items and services is implemented [DCD Ch.17.3].

The reactor uses proven components and systems for power generation; thus operating experience exists to be used also for an optimization process. The reliability of the valve systems to initiate safety related actions should be analysed further.

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 Requirements are addressed.

(a) In section C, the Requesting Party discusses how the radiation risks are evaluated and mitigated in the context of FP8, ST2 and ST3. The standard design will also meet the USNRC Regulatory Guides 1.111, 1.112 and 1.113 on this issue.

(b) The natural and human induced hazards are covered under the site parameters (Table A.1.8-1) of the Head Document. An actual site is acceptable if its site characteristics fall within these site design parameters. Section 2.2 of Design Control Document describes the quantitative criteria to be used for selecting the design basis hazards. In addition to earthquakes, tornado and external flooding, the following human induced hazards will be evaluated for a particular site: explosions, flammable vapour clouds, toxic chemicals, fires and airplane crashes.

(c) The UK requirements on Regulatory Assessment of Siting ST1, ST2 and ST3 are addressed in the DCD. It is also shown to meet the applicable USNRC regulatory guides (1.101, 1.111, 1.112 and 1.113).

The documentation provided allows an assessment of whether the Requirement is addressed. Since the Standard Plant has been certified, the needed information can be found in the DCD, FSER and the SAP Roadmap.

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

Review Results

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

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

The documentation provided allowed an assessment of whether the Requirement is addressed. Since the Standard Plant has been certified, the needed information can be found in the DCD, SER and the SAP Roadmap.

4.24–4.26 Radiological Protection Provisions

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

Review Results

The Requirement is addressed. The design of AP1000 takes measures to control the exposure of people and the releases of radioactive materials to the environment, to restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, and to mitigate the consequences of such events if they were to occur. Further discussion of defence in depth is presented in the assessment of IAEA Draft Requirement 4.45.

The AP1000 design makes use of advanced passive safety features and extensive plant simplifications (A.2) aimed at enhancing safety including the following:

- AP1000 safety features rely on natural driving forces, such as pressurized gas, gravity flow, natural circulation flow, and convection.
- AP1000 safety features do not use active components, such as pumps, fans, chillers, or diesel generators.
- AP1000 safety features are designed to function without active safety support systems, such as AC power, component cooling water, service water, and HVAC.
- Multiple levels of defense-in-depth are aimed at accident mitigation resulting in low core damage probabilities.
- A few simple valves align and automatically actuate the passive safety systems. Most of these valves are designed to actuate to their safe positions upon loss of power or upon receipt of a safeguards actuation signal.
- It is claimed that the AP1000 design meets deterministic safety criteria with large margins. In particular the AP1000 safety features are aimed at maintaining core cooling and containment integrity indefinitely following design basis faults, without a need for operator action or AC power (A.2).

It is indicated in the documentation that the AP1000 safety philosophy provides for three levels of protection:

- Accident resistance
- Core damage prevention
- Accident mitigation

Accident resistance is provided by plant design characteristics, which reduce the dependence on engineered safeguards systems to achieve safety and protect the utility's investment. The AP1000 plant design is aimed at minimizing the occurrence and propagation of initiating events, which could lead to significant events and resulting challenges to safeguard systems. The top-level AP1000 accident resistance measures are as follows:

- Simplification that reduces the chance of failures or leakage that would require a shutdown or cause an accident;
- Proven power-producing component designs that have been optimized using operating experience;
- Increased margin between safety setpoints and normal operation to provide for a more forgiving plant;
- Non-safety features that respond to anticipated transients and automatically keep the plant parameters within their desired values;
- Reactor design with a power reactivity coefficient that is sufficiently negative to support ATWS mitigation throughout equilibrium fuel cycles;
- Use of best available materials and water chemistry, based on the extensive light water reactor operating experience;
- Enhanced man-machine interface system to promote error-free normal operations and quick, accurate diagnosis of off-normal conditions; and
- Proven diagnosis monitoring techniques for leak detection, vibration, and other potential problems to minimize failure of critical rotating equipment and high pressure systems.

The second level of protection is core damage prevention with improvements in engineered safeguards systems.

The third level of protection is mitigation of accidents. The reliability of the containment function is enhanced by:

- Redundant, diverse containment cooling that is primarily based on passive safety system features that can function in a severe accident environment;
- Containment system components that are redundant and sufficiently independent from the systems whose failure could lead to core damage, to avoid vulnerability to common cause failure; and
- Reduced number of penetrations, minimized number of normally open penetrations, and use of fail-closed isolation valves where possible.

As a result, it is claimed that no large release of fission products is predicted to occur from an initially intact containment for more than 100 hours after the onset of core damage. This is assuming no actions for recovery. This amount of time provides for accident management actions to mitigate the accident and prevent containment failure.

In most cases it is predicted that in-vessel retention will be available, which will allow the containment to remain intact indefinitely (A.2).

Significant steps have been taken to increase the level of safety of the AP1000 in comparison to conventional designs. The advantages, potential draw-backs and additional needs for analysis are further discussed under IAEA Draft Requirement 4.45.

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

Review Results

The Requirement is addressed. The measures taken in the AP1000 project are aimed at ensuring that no individual bears an unacceptable risk of harm.
Based on probabilistic risk assessment insights and results, the following design enhancements in addition to safety features of AP 600 have been incorporated in the AP1000 plant:

- Changed normal position of the two containment motor-operated recirculation valves (in series with squib valves) from closed to open.
- Changed IRWST drain procedure to occur earlier for IVR support.
- Improved IVR heat transfer.
- Improved IRWST vents.

The internal Westinghouse design goals are an order of magnitude safer than the thresholds established by US NRC. Due to considerations of optimisation of protection the actual design measures are aimed to go beyond that by reducing the potential severe accident releases and doses to the public to a fraction of the goal values. The optimization of protection in case of severe accidents is implemented by consideration of SAMDA.

In Chapter 33, the plant core damage frequency (CDF) for internal initiating events at power is calculated as 2.41E-07/reactor-year. High pressure scenarios contribute 4.5% of CDF, the remaining cases being scenarios with RCS depressurization (Table 43-1).

Large Release Frequency (LRF) quantification is presented in Chapter 43. LRF is estimated as 2 E-8 /reactor-year, of which containment bypass sequences and early containment failures provide contribution of 44% (Table 43-5).

It should be also observed, that the goal of Westinghouse deals with exceedance of the dose of 0.25 Sv. Learning that the 0.25 Sv dose is exceeded, one does not immediately expect, that it is not 0.25 Sv, but a few hundred Sv, which will be obtained at the exclusion area boundary. According to DCD App. 1B on SAMDA, the contribution of BP sequences to the population whole body TEDE dose risk in 24 hours is 78% and the dose risk is 3.39E-02 person-rem/reactor- year. Evidently the hazard of bypass is the dominant one and all efforts should be directed at reducing containment bypass possibilities.

The issue of containment bypass has been addressed in AP1000 design. AP1000 has, approximately, 55 percent fewer piping penetrations and a lower percentage of normally open penetrations compared to current generation plants. Normally open penetrations are closed by automatic valves, and diverse actuation is provided for valves on penetrations with significant leakage potential. All isolation valves have control room indication to

inform the operator of the current valve position (59.9.5.1). Protection against the failure to isolate the containment and against failure of isolation valves to fully close is described in (59.9.5.2).

The US approach of monetary valuation of health effects is not used by the IAEA. While it is recognized as a possible tool for optimization of protection, the issue of high risk involved in containment bypass deserves further attention in the next step safety report.

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

Review Results

The Requirement is addressed. All conditions and states of AP1000 reactor are considered, starting from normal operation, through anticipated operational occurrences to accident conditions and severe accident conditions both under normal full power and in low power and shutdown state.

The AP1000 design has used both deterministic (DCD Chapter 15) and PRA (DCD Chapter 19, PRA report) considerations to support the claim that core damage prevention is as low as reasonably practicable (ALARP).

The PRA evaluation is made and presented in 59 chapters of the UK AP1000 design acceptance application documents.

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. According to DCD and PRA, the AP1000 system, structure, and components are designed and will be constructed to proven industry and regulatory standards. These standards have been optimized by thousands of reactor-years of operation. The design was analyzed using conservative NRC criteria for design bases events. The analyses were then used as input to the Technical Specification to ensure the plant operation will be reflective of both analyses and design criteria. The design was then optimized, using PRA evaluations. The criteria and process followed by the AP1000 design team show that the issue of reaching the highest level of safety that is reasonably practicable, has been addressed throughout the design.

All recommendations of NRC based on relevant operational experience including TMI requirements have been addressed. This includes recommendations of NRC Regulatory Guides, Compliance with Standard Review Plan (NUREG-0800), Three Mile Island Issues, Review of NRC List of Unresolved Safety Issues and Generic Safety Issues and description of their resolution in AP1000, Advanced Light Water Reactor Certification Issues, SECY-90-016 Issues, Other Evolutionary and Passive Design Issues, Additional Licensing Issues and Operational Experience (DCD 1.9).

Documentation is provided to support the claim that proven power-producing component designs have been optimized using operating experience (A.2) including:

- Core, reactor vessel, and reactor internals which are similar to those of a conventional Westinghouse PWR design with several important enhancements, all based on existing technology (DCD Chapter 4);
- Steam generator design based on proven model Delta-125 steam generator technology with several design enhancements (DCD Section 5.4.2);
- Reactor coolant pump based on proven canned-motor pump technology (DCD Section 5.4.1);
- Turbine generator based on existing technology, with exception to the new design last stage blading for increased performance and efficiency. Full-scale testing of the new design last stage blading configuration and installation in a plant is foreseen to prove the reliability of the machine for the AP1000 (DCD Section 10.2); and
- Materials for components selected based on lessons learned from the operation of existing plants e.g. for reactor vessel, steam generators, and secondary side components (condenser tubes, heat exchangers, and the like) (DCD Section 5.2.3).

Further features addressed which are based on extensive light water reactor operating experience include:

- Use of best available materials and water chemistry;
- Greatly improved man-machine interface system, which promotes error-free normal operations and quick, accurate diagnosis of off-normal conditions; and
- Proven diagnosis monitoring techniques for leak detection, vibration, and other potential problems to minimize failure of critical rotating equipment and high pressure systems.

The plant includes several novel features, which have been tested as described in assessment of Requirement 4.29.

The DCD stresses that the statements about using proven technology found in DCD are supported by the history of Westinghouse activities in nuclear power development which include design, development, and manufacturing of more than 100 commercial nuclear power plants with a combined electrical generating capacity in excess of 90,000 MW. (C.FP2).

The application of existing experience and reliability of testing of new features is addressed in many chapters of DCD.

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

Review Results

The Requirement is addressed. The major plant design objectives are described and the developments in defence-in-depth concept are presented.

The design principles include (A.2):

- Stable operation –to be achieved by the selection of materials, by quality assurance during design and construction, by well-trained operators, and by an advanced control system and plant design that provide substantial margins for plant operation before approaching safety limits (A.2) including:

    - Increased margin between safety setpoints and normal operation;
    - Non-safety features that respond to anticipated transients and automatically keep the plant parameters within their desired values;
    - Pressurizer inventory and steam generator secondary side inventory larger than plants of similar power ratings; and
    - Reactor design with a power reactivity coefficient that is sufficiently negative to support ATWS mitigation throughout equilibrium fuel cycles.

- Physical plant boundaries including high-integrity steel containment pressure vessel to enhance the containment boundary.

- Passive safety-related systems – to be sufficient to automatically establish and maintain core cooling and containment integrity for an indefinite period of time following design basis faults. This is assuming the most limiting single failure, no operator action, and no onsite and offsite AC power sources. AP1000 safety features rely on natural driving forces, such as pressurized gas, gravity flow, natural circulation flow, and convection (C.EKP.3), and do not use active components, such as pumps, fans, chillers, or diesel generators. AP1000 safety features are designed to function without active safety support systems, such as ac power, component cooling water, service water, and HVAC. A few simple valves align and automatically actuate the passive safety systems. Most of these valves are designed to actuate to their safe positions upon loss of power or upon receipt of a safeguards actuation signal.

- Diversity within safety systems – (C.ESS.7) Passive residual heat removal is provided by heat exchanger (PRHR HX) and a diverse passive safety injection and automatic depressurization (passive feed and bleed) functions of the passive core cooling system. The passive containment cooling system includes two trains with water drains and a diverse third water drain valve and drain path (C.SC.5). For control systems, the diverse actuation path extends beyond the cabinet-based

electronics to also include all equipment to the final actuation devices, for example of air-operated valves, squib-operated valves and motor-operated valves (DCD Section 7.7.1).

- Non-safety systems of high reliability should automatically actuate to provide a first level of defence to reduce the likelihood of unnecessary actuation and operation of the safety systems.

- Containing core damage by retaining core debris inside the reactor vessel. In a core damage event where the core has uncovered and overheated, water will flood the outside of the reactor vessel aimed at providing sufficient cooling to prevent reactor vessel failure and subsequent relocation of molten core debris into the containment.

The design principles for accident mitigation are as follows:

- Prevent core/concrete interaction by retaining molten core debris inside the reactor vessel

- Prevent high-pressure core melt sequences by using highly redundant and diverse automatic depressurization valves;

- Prevent hydrogen detonation by using a large rugged containment vessel, igniters, and passive autocatalytic recombiners;

- Prevent hydrogen burning from failing the containment by using a large rugged containment vessel and preventing large standing flames from being too close to the containment;

- Prevent steam explosions from challenging the containment integrity by using highly redundant and diverse automatic depressurization valves and in-vessel retention of core debris;

- Use redundant, diverse containment cooling that is primarily based on passive safety system features that can function in a severe accident environment;

- Use containment system components that are redundant and sufficiently independent from the systems whose failure could lead to core damage, to avoid vulnerability to common cause failure;

- Minimize the chance of failure to isolate the containment by reducing the number of penetrations, minimizing the number of normally open penetrations, and using fail-closed isolation valves where possible; and

- Minimize the chance of containment bypass sequences.

The review of the documentation shows that all these design principles have been addressed.

In general, AP1000 system design uses redundancy features to account for single failure criteria. Diversity is used to address shutdown requirements. Segregation is used to account for fire, flood, and seismic requirements (.EDR.2).

The major plant design objectives are described and the developments in defence in depth concept are presented. Proven power generating system arrangements and components are used to ensure that a plant prototype is not required. The passive safety systems are claimed to require no operator actions for long periods of time (at least 72 hours for design basis faults) (A.3.1)

The next step safety review should confirm fulfilment of all design requirements mentioned in the DCD as listed above.

Aircraft crash withstanding capability needs to be proven. The EUR requires that new plant designs to be built in Europe demonstrate the capability to withstand an aircraft crash. The AP1000 designers, working with the European Passive Plant Groups, have committed to provide a containment design that will be capable of withstanding an aircraft crash without a significant impact to the public health and safety. It is stated that specific analyses and design features will be available by the end of 2007. (A.3.7.5)

The next step safety report should provide information on how this issue has been addressed.

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 addressed. Information is given on the tests conducted during the AP 600 Conceptual Design Program (1986 through 1989) to provide input for plant design and to demonstrate the feasibility of unique design features. Tests for the AP 600 design certification and design program were devised to provide input for the final safety analyses, to verify the safety analysis models (computer codes), and to provide data for final design and verification of plant components. An AP1000 specific Phenomena Identification and Ranking Table (PIRT) and scaling analysis (Reference 25),and a review of safety analysis evaluations of AP1000 (Chapter 15 of this DCD) show that AP 600 and AP1000 exhibit a similar range of conditions for the events analyzed. This provides justification that the database of test information generated during the AP 600 Conceptual Design Program is sufficient to meet the requirements of 10 CFR Part 52 for AP1000. (DCD 1.5).

The new features of the AP1000 checked within the test programmes were:

Core make-up tanks to be drained by gravity in case of LB LOCA and hermetically sealed, high inertia centrifugal canned-motor reactor coolant pumps (RCPs), passive safety injection system check valve flow vs. ΔP with low differential pressure, for small break LOCA - the automatic depressurization system which depressurizes the primary system to near containment pressure including squib valves (C.ERL.1).

Containment Cooling was tested in a large programme, which covered water film behaviour, evaporating heat transfer, containment external cooling air flow path pressure drop, steam condensation heat transfer, integrated behaviour of the steam condensation on the inside, and the evaporative film cooling and air cooling on the outside of a pressure vessel, including wind tunnel tests (DCD 1.5.1.3).

The issue of scaling the results from AP 600 to AP1000 is sensitive and should be further clarified in the next stage of safety review.

The PRHR heat exchanger was tested to check if natural circulation driving forces provide sufficient heat transfer characteristics (CD 1.5.1.4).

In view of the shorter coastdown of the AP 600 canned motor reactor coolant pumps, DNB testing was performed to extend the DNB correlation to the lower flows (DCD 1.5.1.4).

Integral Systems tests were conducted by Westinghouse, a low-pressure scaled test and a full-height, full-pressure test. In addition, the NRC conducted tests in the low-pressure scaled test facility (DCD 1.5.1.).

AP 600 Component Design Tests were performed to confirm their reliability or that materials and fabrication methods meet ASME requirements.

In-core Instrumentation Systems similar to the AP 600 and AP1000 top mounted fixed in-core detector (FID) instrumentation have been demonstrated in operating plants. A test was performed to demonstrate that the system will not be susceptible to electro-magnetic interference (EMI) from the nearby control rod drive mechanisms.

Reactor Coolant Pump/Steam Generator Airflow Test was performed showing no flow anomalies or vortices in the channel head induced by the dual impellers, and Reactor Coolant Pump High Inertia Rotor/Bearing Tests were performed to develop a detailed quantitative knowledge of the factors influencing bearing design and performance (DCD 1.5.2.).

The remaining issue is related to the limited knowledge of physical phenomena related to corium behaviour. The mechanism of external cooling of the RPV with molten corium has been shown to be effective for Loviisa reactor, which has a small RPV containing a low power core (440 MWe). The results were extrapolated to AP 600, and then once again to AP1000. If, however, the external cooling should fail to be fully effective for a large size core and large RPV, the failure of the RPV and the subsequent reaction of corium with water and with concrete would result in a peak generation of steam and then in long term releases of non-condensable gases. Since this would involve unpredicted loads to the containment, the clarification of that issue should be provided in more detail in the next step of the safety review. The capacity of the containment to survive related phenomena and possibly to be vented at full design pressure should be clarified.

For Large-Break LOCA the application of gravity drained tanks for passive heat removal under accident conditions has been a reason for doubts as to whether the system would work reliably at low pressure differences. In particular, the gravity drained core makeup tank is unique to the AP 600 and AP1000 design. A specific AP 600 test was conducted for this component. In addition, a test of passive safety injection system check valve flow vs. ΔP with low differential pressure has been completed. The evaluation shows that these tests are applicable to AP1000 (DCD 1.5.1.1).

For small-break LOCA the core makeup tank tests duplicated small-break conditions as well as the large-break conditions. The automatic depressurization system provides controlled venting of the reactor coolant system to reduce pressure to allow transition to gravity driven injection from the IRWST. Full-scale tests were conducted in the AP 600 test program to simulate the automatic depressurization system, to confirm the capacity of the automatic depressurization system valves and spargers, and to determine the dynamic effects on the IRWST structure. As shown by the AP1000 evaluations, these tests also support AP1000 safety analysis.

Full-scale testing of the new Turbine Generator design last stage blading configuration and installation in a plant is foreseen to prove the reliability of the machine for the AP1000. (DCD Section 10.2, A.2).

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

Review Results

The Requirement is addressed. The classification of structures, systems and components is described and listed in extensive tables [DCD Ch. 3.2 incl. related tables]. The links between SSC and the systems should be outlined in more detail. Also, all the software of the safety-classified programmable I&C should be outlined in more detail.

The classification follows the standard US procedure and thus does not explicitly address the relevant Requirements as formulated in NS-R-1, which are consistent with the formulation of the principles of the UK HSE SAPs. Therefore, there is the need in the next step to review in detail to which extent the classification system used for the AP1000 is implicitly addressing the IAEA Requirements and the SAPs'.

The probabilistic methodology has already been used in the design process from the beginning [DCD Vol. 2 Ch. 19.1]. Based on probabilistic risk assessments, changes to the AP1000 design have been implemented [Head Doc. App. B3]. The dominant core damage sequences were identified using probabilistic analyses [DCD Vol. 2 Ch. 19.59.3.1].

The codes and standards used in AP1000 design are listed in detail [Head Doc. App. B.2].

The reactor uses proven components and systems for power generation; therefore, codes and standards for the AP1000 have been evaluated und used before.

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 addressed. The natural and human induced external hazards are covered under the site parameters (Table A.1.8-1) of the Head Document. An actual site is acceptable if its site characteristics fall within these site design parameters. Section 2.2 of DCD describes the quantitative probabilistic criteria to be used for selecting the design basis events. In addition to earthquakes, tornado and external flooding, the following human induced hazards will be evaluated for a particular site: explosions, flammable vapour clouds, toxic chemicals, fires and airplane crashes. It is noted that the Safe Shutdown Earthquake for the Standard Plant is 0.3 g peak ground acceleration which exceeds the SSE level normally specified for plants in UK (0.25g). Further, the seismic margin goal for the plant is 0.5 g which is also larger than the desired level in UK (0.35g). Following the EUR, AP1000 designs will be designed to withstand the impact of postulated aircraft. This should be confirmed during the site specific review.

The UK system requires a Design Basis Event, which is defined probabilistically, the level of which is usually between 0.1 and 0,25g, dependent on the local seismic history and local site conditions. A seismic margin goal requirement is not defined. Following the EUR, AP1000 will be designed to withstand the impact of postulated aircraft. This should be confirmed during the site specific review.

Since the Standard Plant has been certified, the needed information can be found in the DCD, SER and the SAP Roadmap.

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. Selection of and design for internal hazards are described in response to EHA 14 (Section C: Safety Assessment Principles Roadmap for AP1000 Design Page C-63). These follow the industry standard practice and conform to USNRC regulatory guides. Section 3 of DCD describes how the structures, systems and components will be designed to withstand the postulated internal hazards. Load combinations that appropriately include the design basis external hazards (e.g., earthquake and tornado), internal hazards and operating loads are discussed in Sections 3.7 and 3.8 of DCD.

Since the Standard Plant has been certified, the needed information could be readily found in the DCD, FSER and the SAP Roadmap.

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

Review Results

The Requirement is addressed. The AP1000 design for the RCS follows the ASME III - code and, hence, selection and application of materials are also in line with this code. Therefore, due attention is paid to the behaviour of material under transient and accident conditions.

In addition, the design is such that leak-before-break is achieved. The number of welds is reduced, there are no seam welds in the RPV, and the quantity of stellite has been minimized to reduce the dose on workers. Measures have been taken to reduce the radiation in the belt line. It is unclear whether moulded parts are still used, or that all has been forged or wrought. The material is planned to be followed through plant life, which enables early detection of aging effects.

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

The AP1000 fuel is described in Vol. 2, Chapter 4. All relevant aspects of fuel, cladding and control rod material are addressed. Detailed information is not present, but for all aspects appropriate references (e.g. WCAP-documents) are mentioned.

It is stated in FSER Chapter 4.1 that the maximum average fuel rod discharge burn up will not exceed 62 GWd/tU. However, Section C26 (Safety Assessment Principles) indicates that the region average discharge burn-up will be as high as 60 GWd/tU. These values are not consistent and it is anticipated in the latest UK case that relatively higher average fuel rod burn up might be reached.

Furthermore, burnable absorber rods made of alumina-carbide material will be used to reduce the beginning of life moderator temperature coefficient (MTC). Therefore, the validation of the core analysis computer codes and programs should be assessed in detail by taking into consideration the effect of burnable absorbers, as well as of possible increased burn-up, especially with regard to safety limits of RIA. Finally, a detailed assessment should be performed on the events assumed to be initiated by the presence of burnable absorbers (wear, fretting, risk of mispositioning), etc.

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

Review Results

The Requirement is addressed. AP1000 safety systems, fluid systems, instrumentation and control, and electrical power systems, incorporate self-monitoring features and are redundant. The fail-safe principle has been addressed as further detailed below. All valve positions are monitored and alarmed in the main control room so that any valve misalignment is immediately revealed. The instrumentation and control safety systems use self-diagnostics to reveal faults from the time of their occurrence. The safety-related DC and 1-E AC electrical power system components are monitored and alarmed in the main control room so that any fault is immediately revealed. DCD Chapters 6, 7, and 8, respectively, provide discussions of the safety-related fluid, instrumentation and control, and electrical systems (C.ESS.21).

The minimum number of valves is used for initially aligning the safety systems. ‘Fail-safe’ valves for the system are used for realignment, wherever possible. (A.3.6).

The AP1000 uses passive safety systems to enhance plant safety which reduces potential failure modes (C.EDR.1).

Further evidence of the design, either to be inherently safe or to fail in a safe manner, is discussed in relation to the NRC General Design Criteria required by 10 CFR 50, Appendix A. Specifically, Criterion 23, ‘Protection System Failure Modes’ requires that the protection system will be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (for example, electric power and instrument air) or postulated adverse environments (for example, extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. Compliance to General Design Criteria DC 23 is described in DCD Section 3 (C.EDR.1).

The AP1000 passive design provides a simplified design with less potential failure modes. For passive safety system design, a failure modes and effects analyses was performed as described in DCD Section 6.3. A failure modes and effects analyses was also performed for the instrumentation and control protection and safety monitoring system. See DCD Section 7.2. An extensive PRA analysis, summarized in DCD Chapter 19 and provided in the AP1000 PRA, has evaluated postulated failure modes and has identified plant improvements (C.EDR.1).

Following requirements formulated in Safety System Status Indication (NUREG-0933 Item I.D.3) the AP1000 main control room has been designed to meet the NRC Regulatory Guide 1.47 recommendations, including automatic indication of bypassed and inoperable status of plant safety systems, as described in Appendix 1A.

Plant safety parameters, protection system status, and plant component status signals are processed by the protection and safety monitoring system and made available to the entire

instrumentation and control system via the redundant monitor bus (DCD, Sections 7.5.2 and 7.5.3) (DCD, Sections 7.5.4 and 18.8.2).

The AP1000 leakage detection system detects, locates, monitors, and manages the leakage of fluid that could give rise to a potentially unsafe situation, and supports the concept of leak-before-break for high-energy piping to prevent sudden and catastrophic failure of high-energy piping (DCD Section 3.6, C.EMC.26, DCD Section 5.2.5).

The descriptions of the measures listed above are supported by explanations of the principles of operation of the equipment in question and by references to US NRC regulatory guides, standard review plan or other documents in force.

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

Review Results

The Requirement is addressed. The RCS of the AP1000 is designed according to ASME III, which includes the consideration of transients and fatigue (usage factor).

In addition, the RSC is subject to in-service inspection as described in Vol. 2, Chapter 3, compliance to criterion 32 of the USNRC General Design Criteria (10 CFR50, Appendix A). Such inspection is designed to detect deterioration of materials by various effects. A material properties surveillance program is in place which follows a.o. the shift in the nil-ductility temperature and its consequences for the allowed number of operational transients.

There is a dedicated Ageing Evaluation Program (Vol. 2, Appendix 3D - Attachments B and D), but it is quite limited in scope (addresses IEEE 323 ageing requirements) and not in line with the treatment in present day life extension programs. Such a program often includes 10 - 14 major components of the primary and secondary circuits, including their support structures. Thus, the Ageing Evaluation Program should be more comprehensive and contain a well-defined series of structures, systems and components.

The next step detailed assessment of the AP1000 should confirmed that real vessel material specimen are irradiated, to be able to follow and predict the ageing process (i.e., they are exposed to a higher flux than the actual vessel material).

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

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

Review Results

The Requirement is addressed. Safety-related equipment and selected portions of post-accident monitoring equipment are classified as seismic Category I, (DCD Section 3.2). The DCD also addresses the seismic and dynamic qualification of safety related equipment other than piping, in particular instrumentation, electrical and certain monitoring equipment, active and non-active mechanical equipment (DCD Section 3.10).

DCD Section 3.10 and 3.11 present or reference information to demonstrate that mechanical equipment, electrical equipment, instrumentation and, where applicable, their supports classified as seismic Category I are capable of performing their designated safety-related functions under the full range of normal and accident (including seismic) loadings. Qualification criteria used for each type of equipment are presented or referenced (DCD section 3.10). There is also documentation of the qualification process used to demonstrate the required structural integrity and operability of mechanical and electrical equipment and instrumentation. The methods of meeting the general requirements for the seismic and dynamic qualification of seismic Category I mechanical and electrical equipment and instrumentation applied in AP1000 according to NRC General Design Criteria 1, 2, 4, 14, 23, and 30 are described in DCD Section 3.1.

The AP1000 approach for environmental qualification of Class 1E equipment is outlined in DCD Appendix 3D. This methodology is developed based on the guidelines provided in IEEE 323-1974.

Qualification for equipment in a harsh environment is based on type testing or testing and analysis. Analysis may be used to determine significant aging mechanisms in mild environment applications. Type testing includes thermal and mechanical aging, radiation, and exposure to extremes of environmental, seismic, and vibration effects. Type testing is done with representative samples of the production line equipment according to the sequence indicated in IEEE 323-1974 to the specified service conditions, including margin. The testing takes into account normal and abnormal plant operation and design basis accident and post-design basis accident operations, as required.

Equipment qualification is required by 10 CFR 50, Appendix A, General Design Criteria 1, 4, 23, and 50; Appendix B, Criteria III, XI, and XVII to 10 CFR 50 and 10 CFR 50.49, include Regulatory Guide 1.89, Regulatory Guide 1.30, Regulatory Guide 1.63, Regulatory Guide 1.73, Regulatory Guide 1.100, and Regulatory Guide 1.131. The maintenance surveillance program follows the guidance of Regulatory Guide 1.33. (C.EQU.1). Additional information regarding conformance with each of these regulatory guides is given in DCD Section 1.9 (C.EMT.3).

It is obvious from the above that the classification strictly follows the standard US procedure and thus does not explicitly address the relevant Requirements as formulated in NS-R-1, which are consistent with the formulation of the principles of the UK HSE SAPs. Therefore, there is the need in the next step to review in detail to which extent the classification system used for the AP1000 is implicitly addressing the IAEA Requirements and the SAPs.

The documentation describes a well defined process (see PRA Chapters 7 and 32) for the establishment and application of the AP1000 PRA database.

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

Review Results

The Requirement is partially addressed. Specific design features that will facilitate the decommissioning programme, especially with regard to reduction of radioactive waste and dose limitation, have been highlighted. No detail other than the fact that the detailed design has been simplified and contains less plant items than previous designs has been provided in the submission to support the decommissioning section. Provisions for dismantling the plant have not been described.

The choice of materials; design provisions; limitation of radioactive contamination, etc, have been considered. However, information on the following has either not been included in the submission, or has been considered as outside the scope of the submission:

- Identification and retrieval of a comprehensive suite of design, construction and operational information, documentation and records has not been identified as within the scope of the design submission (DC6).
- Information on the provisions in the site layout to facilitate removal or dismantling of large plant items is not specifically highlighted within the submission for decommissioning.
- Although the various strategies for decommissioning and dismantling are defined within the submission, making of the facility passively safe before entering care and maintenance phase is not considered as within the scope of the design submission (DC5) and no information has been provided within the specific decommissioning section regarding the provisions within the design to allow various dismantling strategies to be adopted.

The information provided could be enhanced with comment on identification, recording and retrieval of construction, commissioning and operating information, and records that would facilitate decommissioning.

It is suggested that information on recording and retrieval of records, site layout provisions for dismantling major equipment and long-term integrity of structures to allow deferred strategies for dismantling, are requested within any future detailed submissions provided.

4.38–4.41 Human Factors

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

Review Results

The Requirement is addressed. Human interactions with the facility or activity are discussed under IAEA Draft Requirement 4.40. The submission addresses the IAEA Requirement for procedures that cover normal operations and anticipated operational occurrences as part of any future combined license application (18.8.2.7, 13.5, and 1.8). Since any procedures will also have to take into account the specific requirements (statutory, legal, organizational aspects, etc) of the national Operating Organization and Regulatory Body, the information provided allows assessing if the IAEA Requirements have been addressed.

However, the submission does specify that Plant Operating Procedures will be developed following the guidance of WCAP-14690 ‘Designer's Input to Procedure Development for the AP 600 Rev1 June 1997’ and APP-GW-GLR-040 ‘Plant Operations, Surveillance and Maintenance Procedures’. The guidance provides input for the development of plant operating procedures, including information on the development and design of the AP 600 emergency response guidelines and emergency operating procedures. (It is stated that they are directly applicable to AP1000 since AP1000 will be operated in the same manner as AP 600).

Procedures will be provided electronically and a back-up system will be available as part of the Human System Interface Design Process (one option is the use of a paper back-up system).

A combined license application will address plant procedures including the following:

- Normal Operation
- Abnormal Operation
- Emergency Operation
- Refuelling and Outage Planning
- Alarm Response
- Maintenance, Inspection, Test and Surveillance
- Administrative processes
- Operation of post-72 hour equipment

The submission does not include information on the development of severe accident management guidance.

The submission recognizes that the development of procedures will require the input of the Operating Organization as part of a future combined license submission. The WCAPs were not provided for review.

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

Review Results

The Requirement is addressed. The submission addresses Competences, Training and Staffing by stating that they will be defined in any future combined license application. However, the staffing requirement assumptions given in the HFE process specify that a single reactor operator should be able to control the major plant functions from the Control Room during normal operations (18.2.1.1).

The submission addresses the Requirement for training (13.2) by stating that any future combined license applicants will develop and implement training programmes for plant personnel. These training programmes will address the scope of licensing examinations as well as new training requirements.

WCAP-14655 ‘Designer's Input to the Training of the Human Factors Engineering Verification and Validation Personnel’ describes the design and implementation of the training programme for operations personnel (18.10). It also describes the process used to develop the specification of the role of the operator for AP1000 and how this role and training insights can be passed from the designer to the developer of the training programmes.

The submission addresses the Requirement of staffing levels and competences of personnel in operations, maintenance, engineering instrumentation and controls, radiological protection, security and chemistry, by stating that this will be addressed in any future combined license application. WCAP 14694 ‘Designer's Input to Determine the AP 600 Main Control Room Staffing Level’ is quoted as a reference. The WCAP is not provided as part of the submission for review.

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

Review Results

The Requirement is addressed. The submission focuses on the process used to design and implement human system interfaces rather than the details of the implementation because of the rapid changes that are taking place in digital computer and graphic display technology (18.1).

The Human Factors Engineering (HFE) design process is designed to meet the requirements of NUREG-0711 'Human Factors Engineering Program Review Model'. The technical disciplines of the Human System Interface Design Team are comprehensive and cover technical project management, systems engineering, nuclear engineering, I&C engineering, architect engineering, HFE, plant operations, computer system engineering, plant procedure development, personnel training, system safety engineering, maintainability engineering and reliability/availability engineering (18.2.2.3). The HFE program addresses the Main Control Room, Technical Support Centre (TSC), Remote Shutdown Room, Emergency Operations Facility (EOF), and Local Control Stations (18.2.1).

The Human System Interfaces (HIS) encompass the instrumentation and control systems that perform the monitoring, control and protection functions associated with all modes of plant normal, off-normal, emergency and accident conditions. Both the physical and cognitive characteristics of the personnel involved in the use, control, maintenance, test, inspection and surveillance of plant systems are considered.

HIS resources include wall panel information, alarm systems, plant information system, computerised procedure system, controls, and the qualified data processing system (18.8).

The design process incorporates a HFE approach in the general plant layout and design (18.8.4.1); this includes maintainability of equipment, accessibility and lay-down areas, lighting, radiation protection and safety, communication, temperature, humidity, ventilation, emergency equipment, storage, and coding and labelling.

Mock-ups of the Main Control Room working areas are utilised as part of the HIS design process. Simulation is utilized to evaluate HFE and HIS issues (e.g. access and conduct of operations).

Information on the provisions in the site layout to facilitate removal or dismantling of large plant items is not specifically highlighted within the submission for decommissioning (Chapter 20).

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 Requirements are addressed. Defence-in-depth (DiD) is addressed in the UK compliance document, Executive Summary. It does not depart from a formal definition, but states that aspects of the design contribute to the DiD.

The text describes, however, mainly the levels 1, 3 and 4 of the DiD-concept. Level 2 is not clear. It is anticipated that level 2 is present, but this requires further analysis of the actual design. E.g., a claim by the Requesting Party is that many non-safety systems preclude actions by safety systems, which can be seen as part of level 2 (and not as level 1, as is stated in the text).

It should be noted that the AP1000 uses also a slightly different formulation for its safety concept than DiD in terms of its three levels of protection: accident resistance, core melt prevention and mitigation of severe accidents. This subdivision of actions can be seen as an important element of the DiD-concept, although not explicitly defined as such.

Level 1 of DiD has been strengthened compared to usual PWR-designs by e.g. eliminating RCP seals, improved SG design, improved material and construction (e.g. forged bends) in the primary system, larger inventory in the pressurizer and SG (to prevent disturbances from the secondary system to open the primary SRVs), leak-before-break for larger lines, reactivity coefficients to cope more easily with ATWS (note: the text talks only on equilibrium cycles, but it should be substantiated in the next step safety assessment that also during start-up - when there is the most risk of disturbances and transients - sufficient protection is available)[1] and better man-machine interfaces. Also in this level is a layout of the RPV and SG so that 1 SG is sufficient to remove decay heat by natural circulation.

Several items have been found in level 2 of the DiD. For example, the robust connection to the external grid, which makes the plant less sensitive to disturbances from its turbine-generator, the possibility for 100% load rejection and the possibility to run only house load (‘island operation’). However, such designs must be thoroughly tested, as many incidents have been reported where these functions failed. The documentation did not reveal such tests or the feedback from past incidents in this area.

In level 3 of DiD, improvements are claimed on the basis of a more passive concept of safety systems, which even eliminates operator actions to mitigate design basis events. Other systems have been added, such as an automatic depressurization system (ADS), much like a BWR, and a passive containment cooler to carry decay heat out from the containment. High- pressure safety injection has been retained, which is a good feature for PWRs, as it allows injection at or close to normal operation pressure and makes successful injection independent from such a complicated transient as a full system depressurisation[2]. Also the LBLOCA has been retained for ECCS design, even if leak-before-break has been

[1] If the moderator temperature coefficient (MTC) is not negative during start-up, compensation can be sought in starting up with Doppler-banks partly inserted, but this is not a favourable core configuration.

[2] Some advanced designs have deleted the high-pressure safety injection.

established on larger lines. On the other side, total reliance on relatively small driving forces as are associated with passive features (notably gravity) must be thoroughly substantiated, otherwise the claimed DiD level 3 protection is not present, e.g., check valves may stick in the closed position, lines may be blocked by debris or the charges of squib valves do not function (recommended for detailed review in the next step of assessment). In the past, substantial incidents have been noted with squib valves, and it became not clear to the reviewers that all these concerns have been resolved in the proposed design.

Other notable features in level 3 are the absence of a loop seal in the main coolant piping, a lay-out that prevents ECCS spill during LOCA and core uncovery from vessel leaks.

As a whole, the concept in level 3 is advanced and should, if sufficiently validated, bring about a major improvement over existing designs. Note that the condition of sufficient validation is essential: without it, the concept loses much of its benefits - if working at all. In this respect, the SAMDA-option to include an active HPSI has been rejected (Vol. 1, Attachment B.4, item 5) on the basis that it is not consistent with the AP-1000 philosophy. The reviewers did not find other arguments which could support this decision - it should be subject of investigations in the next step safety assessment. Note: item (3) in sec. 5.32 of the IAEA Requirements on Design requests such design improvements to be implemented, if reasonably practicable.

For severe accidents (level 4, DiD), the claim is that water from the IRWST will prevent RPV melt-through. The evidence known to the authors is that such mechanisms are effective for power levels up to about 600 MWe (e.g. by investigations for Loviisa, Finland). Hence, the statement would be applicable to the AP 600. The claim that the mechanism is also effective for the AP1000 must be thoroughly substantiated, otherwise the whole concept of severe accident mitigation of the AP1000 will fail, as the passive safety features of the AP1000 are incompatible with basemat melt-through. The arguments in support of this claim, as has been reiterated in Vol. 2, sec. B.2.1, are documented in Vol. 2, Chapter 19, sec. 19.39 ff. An important argument here is that the debris pool consists of a metal layer over an oxide layer. In the OECD RASPLAV and MASCA projects, such configurations have been studied in detail, and it was concluded that the configuration depends much on the composition of the pool and no generic statement on its composition can be made in advance. The AP1000 submittal does not refer to these newer insights. Hence, the documentation of its safety case is not complete and it is recommended to investigate this matter further in the next step detailed safety assessment.

Another consequence of the concept is the absence of any containment vent, filtered (many European applications) or unfiltered (US-applications). The reviewers are of the opinion that the absence of such a vent - for reactors which may generate substantial masses of non-condensables after RPV melt through[3]- should be thoroughly investigated in the next step safety assessment, also in the light of (3) in sec. 5.32 of the IAEA Requirements on Design, which asks for design changes for prevention or mitigation of severe accidents, if these are reasonably practicable.

[3] The amount of gas depends on the type of concrete

In addition, a severe accident cannot be considered to be under control as long as not all debris is covered and cooled, which requires flooding of the containment to a level above top-of-active-fuel (TAF). No provision has been found to enable this process. Usually, under SAMG execution, a containment vent is used to mitigate the associated rise in containment pressure. As the core is located relatively low in the containment, no substantial rise of containment pressure is, however, expected.

Notable features are the dedicated actions to prevent direct containment heating (DCH) and measures against hydrogen accumulation. It should be noted that the presence of non-condensables will influence the working of the passive containment cooler. The review could not confirm that such influence indeed has been considered to its full extent (Vol. 2, Chapter 19, sec. 19.40). Note that the occurrence of RPV melt-through generates even more non-condensables, and that it would be prudent - even if such melt-through is a low probability event - to include it in the design of the passive containment cooler. In other words, DiD level 4 margins must be clearly established or otherwise alternatives should be sought. This matter should be further investigated in the next step safety assessment.

Regarding hydrogen generation, even where the AP-1000 containment is a relatively open construction, the risk of H2 accumulation has been studied for the containment, together with the associated phenomena like flame acceleration and DDT (Vol. 2, Chapter 19, section 19.41). The AP1000 design recognizes the difficulty in this area in sec. 19.41.2, quotation: “The maximum dynamic loads from accelerated flames and detonations are difficult to calculate”. Review calculational tools and their validation should be addressed in the next steps of the GDA process.

In addition, Vol. 1, sec. A.3.4.3 states that the PSA has been used for hydrogen control. The review team could not establish what was meant. Care should be exercised so as not to eliminate otherwise useful strategies from the design on the basis of perceived low probabilities. Hydrogen management should be robust, and not dependent on finely tuned probability considerations. A detailed assessment is needed to come to a firm conclusion, which should be part of the next step safety assessment.

Other issues relevant for severe accident management are the inclusion of a remote shutdown station (also relevant for area events), the habitability of the main control room (MCR) during a severe accident, and the availability of a Technical Support Centre (TSC). These are relevant, if not essential items for such management. A remote shutdown station is present, as is a TSC (although the information on the latter is not unique: a TSC can be provided if required (Vol. 2, sec. 1.2.5)). The MCR is equipped for protection against DBA (Vol. 2, sec. 1.9.3, item (2) (xxviii), which may not be sufficient to also offer protection against severe accidents. As the MCR and TSC share HVAC equipment, this situation may also exist for the TSC. The next step detailed assessment should investigate the use of the MCR and the TSC during severe accidents.

A notable feature for DiD is also the feedback from the PSA into the design before the design is finalized (Vol. 1, sec. A.3.4.3, and Attachment B.3). An important change is the logic to eliminate the possibility of SG overfill during SGTR (based on the typical Westinghouse policy of an early isolation of the affected SG, in contrast to other designs that focus on primary depressurisation and later isolation). However, it could not be established whether additional Postulated Initiating Events (PIEs) have been found which

should be incorporated into the design. This should be further investigated in the next step detailed assessment.

In addition, a number of BDBAs are relevant, which formally are accommodated under DiD level 4. It did not become clear which ones have been studied and for which ones protection has been incorporated in the design. Systems relevant for the protection against these events usually include normal operational systems, but their role in mitigating BDBAs has then been identified and the systems have often been given a special class for design and operation. Such specific classification has not been found here. (The use of such a classification could be inferred from the classification Requirements of IAEA NS-R-1 and has thus been included into IAEA DS 367, i.e. the draft safety guide NS-G-1.14.) Only a limited 'availability control' was established (Vol. 1, sec. A.3.4.6). Similarly, the Technical Support Centre is considered not to be safety-relevant ((Vol. 1, sec. A.3.6, last line), which is remarkable in view of the function this centre has. These items should be evaluated in the next step detailed assessment

Various severe accident alternatives ('SAMDAs') have been studied - none found meeting the cost-benefit criteria (Vol. 1, sec. A.3.5.2). The results, however, depend very strongly on the value of risk aversion. E.g., in many studies originating in the US, a value of $ 100 per man-mSv ($ 1000 per man-rem) averted is taken as a basis. The conclusion of the reviewers is, hence, that the safety case for severe accidents is not yet complete: IAEA Requirements on Design, sec. 5.32 item (3) requires the implementation of such design features, if reasonably practicable. 'Reasonably practicable' in European candidate countries could mean other acceptable values - where such values exist. Notably the deletion of the containment spray system warrants further investigation, as this is more or less the only system which would be able to mitigate containment bypass events. These items should be further investigated in the next step detailed assessment.

Severe accidents also require appropriate accident management procedures or guidelines, usually known under their acronym SAMG (Severe Accident Management Guidance). Such guidance deviates from Emergency Operating Procedures (EOPs), as it focuses fully on the protection of the (remaining) fission product barriers, eventually without taking notice of the protection of the plant itself. As an example, a relevant issue for SAMG may be the starting time of the passive containment cooler, as it contributes to de-inertisation of the containment atmosphere. A framework for SAMG has been set up (DCD, sec. 19.59). The development of a complete set of SAMG already at this early stage is a very beneficial item in the DiD level 4. In the next step assessment it should be investigated whether it meets the recommendations of the (draft) IAEA Safety Guide on Severe Accident Management, DS385.

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 AP-1000 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 AP-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 AP-1000 concept bases largely on passive safety systems. Although this gives clear advantages, there is also a risk that the driving forces are too small to overcome blockages and sticking check valves. Also the reliability of squib valves should be further investigated.

The DiD-concept in the AP-1000 should be carefully analysed, notably where important deviations occur from established practices, as discussed above. Also the margins believed to be present in the severe accident domain need a careful analysis, as some margins may not have a solid basis in the present-day understanding of severe accidents. If the in-vessel retention cannot be fully substantiated, the concept loses much of its value. The SAMDA analysis should be checked against NS-R1 for ‘reasonable practicable’ design changes and may need adaptation to European standards, where available. Examples of items to be studied are the use of the HPSI, the containment vent and the containment spray system. Further recommendations for the next step safety assessment are referred to above.

4.49–4.52 Scope of safety analysis

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

Review Results

The Requirement is addressed. The information on the safety analyses performed for the various operational states of the reactor is provided in Chapter 15 of the DCD. Radioactive releases from a subsystem or component are included in the analysis.

Regarding the post-operational state, DCD Chapter 20 provides summary information on decommissioning. Three stages of decommissioning and different decommissioning strategies are described. The chapter includes a summary of the inventory of contaminated material after different periods of decay. Design features aimed at minimizing radioactive waste are briefly summarized.

Compliance with US NRC Regulatory Criteria including 'Three Mile Island Issues' and the list of 'Unresolved Safety Issues and Generic Issues' is systematically addressed in DCD Chapter 1.9. The AP1000 has undergone the US NRC design certification process. The NRC Final Safety Evaluation Report for AP1000 Design is appended as Section F of the documentation. It is stated that there are no open items.

Document 1 Section C 'Safety Assessment Roadmap for AP1000 Design' provides information on how the results of safety analyses described in the DCD and the PRA, aimed at demonstrating compliance with the NRC criteria, address the SAPs of the UK HSE.

Document 1 Section D 'Western European Nuclear Regulators' Association Roadmap' provides a description on how the design complies with the WENRA safety reference levels. It is stated that the design meets the WENRA requirements.

Section B of Document 1 summarizes information on how the design addresses the US Advanced Light Water Reactor Utility Requirements (URD) and the European Utility Requirements (EUR).

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

Review Results

The Requirement is addressed. Consequences of normal reactor operations and surveillance are estimated in DCD subchapter 12.4.1.7 for occupational exposure (67.1 man-rem) and in subchapter 11.3.3.4 for the site boundary at ground level (2.1 mrad for gamma, 10.1 mrad for beta radiation).

Results of the accident analyses are presented in DCD Chapter 15 and Chapter 19 (PSA results) and the separate PSA documentation. However, the analyses follow the standard US NRC procedure based on a classification of plant conditions into the categories I to IV. Also, for calculating radiological consequences the standard NRC procedure is followed. In order to address these differences from the categories of the IAEA standards and the more detailed SAPs, Document 1, Appendix C, 'Safety Assessment Principles Roadmap for AP1000 Design', provides information on how the events treated in plant conditions I to IV relate to the categories of fault sequences contained in the SAPs of the UK HSE.

Initial startup testing programmes are described in DCD Chapter 14. This includes the tests to be performed for the first of a kind plant. These test results will be used to verify parameters for the performance of innovative safety features.

In addition to the design basis accidents the accident analysis includes, consistent with NS-R-1, specified accidents beyond the design basis, including severe accidents. Best estimate analysis is performed in this category.

The frequencies and consequences of severe accidents are analysed in the full scope Level 1, 2, 3 PSA, including low-power and shutdown modes and internal and external events. Depending on the complexity and uncertainty in processes bounding assumptions are used.

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

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. 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. 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.

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).

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”.

Review Results

The Requirement is addressed. As described in Document 1 Chapter A.3.3 and DCD Chapter 15 the selection and grouping of anticipated operational occurrences and accident conditions within the design basis follows the standard US NRC procedure. It is stated that “the basic principle applied in relating design requirements to each of the conditions is that the most probable occurrences should yield the least radiological risks, and those extreme situations having the potential for the greatest risk should be those least likely to occur”. Internal and external events are included. In line with the rules of a deterministic safety analysis partial or complete failure of components is assumed. Conservative bounding assumptions are made.

Many tests have been performed for the AP 600. DCD subchapter 1.5 provides information regarding scaling of the AP 600 test data to AP1000 conditions. It is claimed that “AP 600 and AP1000 exhibit a similar range of conditions for the events analysed” in the safety analyses. Table 1.5-1 provides an extensive list of related Westinghouse Topical Reports. In particular, reference is made to a topical report ‘AP1000 PIRT and Scaling Assessment’ which could not be included into the review at this stage.

Large-break LOCA is included as a condition IV event (limiting fault) and postulated as a conservative design basis. The accident analyses make use of the WCOBRA/TRAC computer code to perform best-estimate large-break LOCA analyses. In accordance with US NRC requirements specified conservative analyses are presented to demonstrate the performance of the containment.

Severe accidents are analysed by using best-estimate methodology. In case of large uncertainties in phenomenological processes conservative bounding assumptions should be made.

Summary information is given on the functioning of the reactor pressure vessel as a heat exchanger during core melt accidents by cooling of the outside of the vessel. DCD subchapter 5.3.5.1 makes reference to the test programme (ULPU Configuration V) with full-scale AP1000 geometry modelling of the water flow between the reactor vessel and the reactor vessel insulation.

The process of using PSA to analyse severe accidents is described in DCD Chapter 19 and the separate PSA documentation. The selection of the list of initiating events is based on a systematic process as described in Chapter 2 of the PSA documentation. The list includes large-break LOCA and RPV rupture, which are then shown to contribute significantly to CDF. The in-vessel retention of molten core debris is summarized in DCD Chapter 19.39. The performance of the passive containment cooling is described in Chapter 13 of the PSA. However, more information should be provided regarding the cooling processes inside the vessel.

While a separate PSA has been conducted for AP1000, some parts of the PSA are developed upon the models or results (minimal cut sets) of the AP 600 PSA with considerations of the design differences. It is therefore an important issue to assess to which degree the similarity of both designs allow extrapolating the approaches or models of the AP 600 to the AP1000.

Summary information only is provided at this stage regarding the processes for in-vessel retention of molten core debris. The experimental basis and more detailed analyses contained in the references will need to be reviewed at the next stage.

Due to the estimated low CDF, LOCA initiating events including RPV rupture contribute significantly; large LOCA 18.7% and RPV rupture 4.2%. It is thus important to review the basis for these initiating event frequencies at the next step.

4.53–4.55 Approaches to Safety Analysis

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

Review Results

The Requirement is addressed. The AP1000 design intends to meet well established deterministic safety and probabilistic risk criteria with large margins, as is concluded from statements in sec. A.1.1 of Vol. 1 (p.A-1). It is further stated that the PSA is being performed interactively with the design, analysis and operating procedures, according to Vol. 1, sec. A.3.4.2 (p. A-65). Examples are presented in Vol. 1, sec. A.3.4.6.

For the deterministic analysis, the FSER, Chapter 3 describes the NRC evaluation, which concludes a.o. that the criteria of NRC's quality group classification are addressed (Reg. Guide 1.26). Criteria of other Standards re classification, such as the ANSI/ANS 58.14 and the draft IAEA Guide NS-G.1.14 go beyond the recommendations of RG 1.26. The review team did not assess whether these higher-level and more elaborate criteria also are addressed and this should be part of the next step safety assessment.

According to Vol. 1, sec. A.3.4.3, the PSA has been used to optimise the design. As such, the integrated decision making process should have been achieved for the AP1000. The next step safety assessment should provide the necessary evidence on the basis of more detailed documentation, including the PSA.

Criteria of other standards /guidelines re classification, such as the ANSI/ANS 58.14 and the draft IAEA Guide NS-G.1.14 go beyond the recommendations of RG 1.26. It is highly recommended to also apply these other documents and investigate potential non-compliances which are relevant for risk and/or Defence-in-Depth.

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

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

Review Results

An overview of the approach, scope, criteria and output of the deterministic safety analyses is presented in section A.3.3 of the UK Compliance Document for AP1000 Design. Further detail is presented in chapter 15 of the AP1000 safety, Security and Environmental Report. For all events considered, design requirements are specified and radiological criteria assessed. The next steps of the GDA process should include detailed review of the calculational models and criteria used in the analyses.

Vol. 2, sec. 3.1.1 states that the QA program for the AP1000 provides confidence that safety-related items and services are designed, procured, fabricated, inspected, and tested to quality standards commensurate with the safety-related functions to be performed.

The FSER, Chapter 3, describes the NRC evaluation, which concludes a.o. that the criteria of NRC's quality group classification are met (Reg. Guide 1.26). Consequently, a number of deterministic rules and requirements are addressed, in accordance with Requirement 4.54.

Criteria of other Standards re classification, such as the ANSI/ANS 58.14 and the draft IAEA Guide NS-G.1.14 go beyond the recommendations of RG 1.26. The review team did not assess whether these higher-level and more elaborate criteria also are addressed. Reference is only found to ANSI N 18.2 and ANS 51.1, both of which have been superceded (Vol. 2, sec. 3.2.2.2).

Certain equipment is designed to prevent actuation of safety systems: class D. As discussed under the assessment for Defence-in-Depth, this level strengthens level 2 of the DiD.

In addition, systems are available to mitigate the consequences of BDBA, not being core melt accidents, and core melt accidents. For the non-core melt accidents, Vol. 2, sec. 17.4 specifies certain requirements, in conjunction with the D-RAP (Design Reliability Assurance Program). For core melt accidents, class D is specified.

Clear design requirements for these classes (e.g. equivalent to DBA), however, were not found. Normal industry standards are used (Vol. 2, sec. 3.2.2.6).

Vol. 1, sec. B.2.1 (forelast bullet), discusses NRC oversight on items with a limited safety mission. However, there is no reference to the control/mitigation of BDBAs/severe accidents in this section.

The assumptions considered for some transients appear as to be non conservative (e.g.: Feed water system pipe break in DCD (15.2.2.8)) in particular regarding the low

pressurizer safety valve set point and the non safety related pressurizer spray. Although some justifications have been provided, this issue should be checked in detail in the next steps.

The conservatism of the demonstration for high burnup fuels should be developed in more details (15.2.4.8 Spectrum of RCCA ejection accident).

The ability of the NOTRUMP code to conservatively predict the liquid entrainment within the upper plenum, hot legs and ADS- Valves in case of SBLOCA should be checked in detail.

The conservatism of assumptions on aerosols removal coefficients have to be confirmed with regard to the LOCA radiological consequences (DCD 15.3.6).

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.

4.55 The aim of a probabilistic safety analysis shall be to determine all significant contributors to the radiation risk from a facility or activity and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where they have been defined. In the area of reactor safety, the probabilistic safety analysis that is carried out uses a comprehensive, structured approach to identify failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. The probabilistic approach uses realistic assumptions whenever possible and provides a framework for addressing many of the uncertainties explicitly. Probabilistic approaches may provide insights into system performance, reliability, interactions and weaknesses in the design, defence in depth and risk that it may not be possible to derive from a deterministic approach.

Review Results

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

Detailed information on the PSA is provided in UKP-GW-GL-022 Rev.0: UK AP1000 Probabilistic Risk Assessment. The document is comprehensive and displays a systematic probabilistic analysis of the design with sufficient scope and level of detail. Overall it appears that the PSA follows internationally recognized practices and procedures and addresses the IAEA recommendations provided in the draft Safety Guides DS 394 and 393 on Level 1 and 2 PSA, with the limitations associated with a PSA performed during the design process. The PSA scope covers Level 1, 2 and 3 analyses for internal initiating events, with several limitations. Low power and shutdown operational states are analysed only in the Level 1 PSA. Level 2 is performed using the so called Risk Oriented Accident Analysis Methodology and is limited to eight phenomenological severe accident issues. Level 3 PSA is limited to an off-site dose evaluation. The scope of hazards considered is limited to internal floods and fires and earthquakes (seismic margin assessment). External hazards, such as tornadoes, hurricanes, external floods, transport accidents, etc. are addressed in the PSA study but excluded from the analysis on the basis that the plant site should be such that the frequency of hazards with a magnitude sufficient to challenge the safety of the plant is below 1E-6/reactor-year. Some parts of the PSA use directly the PSA for the AP 600 or are developed upon the models or results (minimal cut sets) of the AP 600 PSA with some considerations of the design differences. It is therefore an important issue to assess to which degree the similarity of both designs allow extrapolating the results or models of the safety assessment of the AP 600 to the AP1000.

The PSA was presented with the application for design certification in the USA. It claims to be in compliance with the US NRC safety goals with significant margins and a balanced risk profile. The overall conclusions are presented in Section 1.1.5 with more detailed information and quantitative figures in other sections of the report.

Based upon the observations presented below and other insights gained during the review, it can be concluded that there is reasonable evidence that this Requirement as well as the associated Requirements of NS-R-1 are addressed, but a more detailed review of the PSA will have to be performed at the next step of the review.

The initiating event (IE) analysis shows a systematic and reasonable process for identification of initiating events, based on previous analyses experience of LWR

operation, previous PSAs, and the analysis of the AP1000 master logic diagram and potential failures in front line and support systems. The initiating events are grouped into categories which have similar mitigation requirements. Three different primary categories are distinguished: LOCAs, transients and ATWSs, the later corresponding in fact to consequential initiating events. Success criteria of safety functions for each group were established based upon extensive accident analysis calculations.

IE group frequencies are estimated in a number of ways, such as generic information and data sources, review of operational LWR experience, with consideration of the number of sections, sizes and other factors for pipe break frequency calculations. Other calculations account for component breaks and failures, human intervention and surveillance processes. The calculations are reasonably well documented in Appendix 2A and 2B.

The accident sequences are well developed and documented, with due consideration to plant response and timing of events, human intervention and available times, dependencies and success criteria. These are in general not best estimate success criteria. Consideration is also given to the interaction of active and passive systems. Dominant sequences leading to core damage are grouped into core damage categories for the interface with the level 2 PSA.

Guidance is provided for the consistent development of fault trees in the analysis of safety systems. The analysis of safety systems is summarily presented. It addresses system dependencies, modes of operation, performance during accident conditions, success criteria, boundary conditions and assumptions, human interactions and common cause failures. Maintenance and testing, associated also to technical specifications is treated in a simple manner, using global assumptions. Values used for surveillance test intervals are not included in the documentation.

The study includes procedures for dependent failures. Common cause failures are postulated for redundant components with little consideration of plant specific root causes, coupling mechanisms and defensive measures in the calculations. Some common cause failure probabilities appear to be excessively low, but a verification of the analysis is out of the scope of this review.

Human reliability analysis is carried out on the basis of the THERP methodology. It is indicated that most of the actions modelled are of type C. No documentation for other type of actions was found. A number of performance shaping factors, aspects of dependency and between actions, procedures and time available are considered in the analysis. The new man-machine interface features of the AP1000 should be considered in the values and curves of the THERP methodology.

The reliability data used should be better documented. The default data source is *Advanced Light Water Reactor Requirements Document*, Volume III, Appendix A to Chapter 1 and PRA Key Assumptions and Ground Rules, Revisions 5 and 6, December 1993. This is a document prepared for EPRI, which is also used for the ESBWR design. Otherwise a number of old generic data sources, like the IEEE Std. 5000 based on ‘expert judgement’, are used. ‘Westinghouse data’ is used for logic and instrumentation data for microprocessor based components. The default data source is also used to assign

unavailabilities due to maintenance and testing to different types of equipment. Since the default data source does not consider uncertainties in failure rates, the uncertainties of failure rates in other documents are taken. While there must be some understanding for the difficulties in gaining reliability data for a new type of reactor, it seems that this part of the analysis is not well documented and some rather old generic data sources have been used.

PSA level 1 quantification is a rather automatic process. No indication of truncation criteria used is given. It appears that no house events have been used. This involves a proliferation of system models for addressing scenario specific conditions, which could not be seen in the system analysis documentation.

The level 2 PSA analysis is limited to eight phenomenological severe accident issues, which are treated using the so called Risk Oriented Accident Analysis Methodology. LRF is calculated for seven fission product release category yielding an average containment effectiveness of 91, 9 % in preventing a large release after core damage. Major contributing scenarios such as SGTR are identified and a number of sensitivity analyses with respect to human intervention, design features and analysis issues, e.g. on sequence binning, are performed, to characterize the uncertainty of the results. From the calculated source terms for each release category off site consequences are estimated and compared with US goals. Code MACCS2 is primarily used for dose evaluation

The LPSD PSA is developed from the minimal cut sets of the LPSD PSA of the AP 600 through a process for making the necessary changes for reflecting the AP1000 design and operation. IE frequencies and CCFs probabilities of PRHR AOVs are modified. Other values of CCFs and human error probabilities were not changed since the AP 600 values were considered more conservative. The result of 1.23E-07/reactor-year for CDF is considered conservative in the analysis. The results of the level 2 PSA for the AP 600 are directly applied to the AP1000 to obtain a LRF of 2.05E-08/reactor-year. Some sensitivity analyses performed, e.g. on the allowed outage of one IRWST injection train, or non taking credit for standby non-safety systems, raise CDF by factors of 18 and 10''' respectively (without considering truncation errors). This is a peculiar probabilistic assessment. The low risk results obtained put an important question mark of the similarity of the AP 600 and AP1000 design for extrapolating the results of one PSA to the other and why, if acceptable, this is only done for the LPSD PSA and level 2 PSA of shutdown states.

The analysis of internal floods and fires is based on the analysis for the AP 600. The impact of fires on human actions is considered for some fire scenarios, but not for floods. Fire PSA follows the FIVE methodology. Several aspects of this methodology are considered nowadays controversial or inadequate. The use of an average combustible load (44% due to cables and 39% due to ‘paper’) per surface unit is not a realistic assumption. Typically important plant areas, such as cable spreading rooms seem to have been screened out or cannot been identified in the list of retained areas. Chapter 59 of the PSA indicates that “In order to minimize potential uncertainty in the results arising from the lack of as-built equipment location and cable routing information, a bounding approach to quantification was taken in accordance with the reference methodology”. Even considering that all equipment in an area affected by fire are damaged, the total fire risk estimate is as low as 5.6E-08/reactor-year for power operation. Therefore, the fire analysis requires a detailed review.

4.57 Criteria for judging safety

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

Review Results

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

Criteria defined by the designer: It is stated that the design is based on the US Advanced Light Water Reactor Utility Requirements Document (URD). The document contains detailed requirements for passive designs. It is stated that these requirements were developed concurrently with the AP 600 design. Many of the analyses have originally been performed for the AP 600. The documentation provides information in DCD subchapter 19.34 and PSA Chapter 34 on how these results have been extrapolated to the AP1000 design. This includes references to publications and reports which were not available within the framework of this review.

The information presented by the designer in the DCD report strictly follows the US NRC procedures and standard format. DCD Chapter 1.9 systematically addresses compliance with US NRC Regulatory Criteria including ‘Three Mile Island Issues’ and the list of ‘Unresolved Safety Issues and Generic Issues’.

The basic safety approach to the safety of the AP1000 is deterministic. The accident analyses include an assessment of the radiological consequences in accordance with US NRC requirements. As a conservative approach to containment performance major core degradation and melting is assumed though the analyses show that core integrity is maintained.

The Level 1, 2, 3 PSA including external events and shutdown risk has been performed to optimise the design and to demonstrate compliance with the US NRC safety goals.

The AP1000 has undergone the US NRC design certification process. The NRC Final Safety Evaluation Report for AP1000 Design is appended as Section F of the documentation. It is stated that there are no open items.

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

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

Due to the difference in concepts the results of the accident analysis by the designer following US NRC standard procedures are not directly comparable to the criteria used by the UK regulator. In order to address these differences Appendix C, the SAP road map for AP1000 design, provides information on how the events treated in plant conditions I to IV relate to the categories of fault sequences contained in the SAPs of the UK HSE.

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

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

4.58–4.59 Uncertainty and sensitivity analysis

4.58 The safety analysis incorporates, to varying degrees, predictions of the circumstances that will prevail in the operational or post-operational stages of a facility or activity. There will always be uncertainties 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.

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.

Review Results

The Requirement is addressed. The core design takes into account all major uncertainties [DCD Vol. 2 Ch.4.4.2.9]. For the containment design available margins are presented [DCD Vol. 2 Ch.6 Tab. 6.2.1.1-1].

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

The core damage and large release frequencies are based on conservative assumptions in specifying success criteria for passive systems [DCD Vol. 2 Ch. 19.59.1].

Severe accident phenomenological uncertainties are treated with the Risk-Oriented Accident Analysis Methodology (ROAAM) [DCD Vol. 2 Ch.19.39.2].

Sensitivity studies are reported at-power and shutdown core damage [DCD Vol. 2 Ch. 19.59.3.8 and 19.59.5.3].

Scaling considerations regarding the AP 600 and AP1000 mainly for the containment, for the passive cooling systems and the severe accident phenomena should be presented for review at the next step.

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. Most components of the AP1000 are based on proven designs. However, several novel safety features have been implemented [UK Compliance Doc.Ch.A.1.1; Ch.A.1.2.5.1-4].

The codes for the thermal-hydraulic, neutron and fuel design are given [DCD Ch.4, Tab. 4.1-2]; code validation is not presented – it is referred to references [e.g. for fuel rod performance see Ch.4.2.33]. It is not clear if the codes calculating the fuel data, the fuel rod and the core behaviour are validated for high burnups.

The potential for and the consequences of Severe Accident phenomena are evaluated; analysis methods and Severe Accident analyses are intentionally not presented [DCD Ch. 19.34 and Ch.19.39]. MAAP4-, NOTRUMP- and MAACS2-codes are used for the PSA.

The ability of the NOTRUMP code to conservatively predict liquid entrainment within the upper plenum, hot legs and ADS-valves in case of SBLOCA has to be discussed in depth [DCD 15.6.5. B 2.1].

The validation of the fuel data, rod and core behaviour for high burnup should be confirmed.

The validation of Severe Accident codes should be outlined.

4.61 Use of data from operating experience

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

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

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

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

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

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

Review Results

The Requirement is addressed. Although this IAEA Requirement is written for an operating nuclear facility and could be considered as not applicable at the design stage, the submission addresses the utilization of Operating Experience and Lessons learned in developing the design. It does not consider the Requirement to collect operating experience and other lessons learned throughout the life of the plant as the responsibility of the designer – it states that this responsibility is clearly with the operator. (Section D, J1 – 4)

Throughout the submission there are many references to utilizing operating experience from operating NPPs to enhance the design.

The Westinghouse Quality Management System (Section E -5) details actions to be taken during design and construction regarding the identification and correction of conditions adverse to safety.

Examples of proven power-producing component designs, (Section A-2) which have been optimized using operating experience are:

- Core, reactor vessel, and reactor internals: The core, reactor vessel, and reactor internals of the AP1000 are similar to those of a conventional Westinghouse PWR design. Several important enhancements, all based on existing technology, improve the performance characteristics of the design. Fuel performance improvements include the use of zircaloy grids, removable top nozzles, and longer burnup features. Fuel performance improvements include ZIRLO™ grids, removable top nozzles, and longer burnup features. The AP1000 core design provides a design with at least 15 percent in departure from nucleate boiling (DNB) margin.

- Steam generator: The AP1000 design uses two model Delta-125 steam generators. The steam generator design is based on proven steam generator technology that includes design features incorporated in the latest Westinghouse replacement steam generator designs.

- Reactor coolant pump: The AP1000 reactor coolant pump is based on proven canned-motor pump technology, which has been used in commercial and naval reactor applications. The reactor coolant pumps do not have seals. This eliminates the potential for seal failure LOCA, which enhances safety and reduces pump maintenance.

- Materials: Materials of construction for components in the AP1000 have been selected based on lessons learned from the operation of existing plants. It is claimed that thus material problems in the AP1000 are prevented. This operating experience has resulted in specification of improved materials in primary system components, such as reactor vessel, steam generators, and secondary side components (condenser tubes, heat exchangers, and the like).

Westinghouse has reported in WCAP 15800 that the NRC has investigated the use of operational data for the AP1000 design and concluded that “the applicant has adequately addressed the inclusion of operational data in the design” (Chapter 20, Generic Issues).

Operating experience will be fed back according to the TMI-action plan (NUREG 0737), as stated in sec. 13.5.3.3. The focus here is, however, on operating procedures.

Data collection as addressed in the Requirement was not found in the documents submitted, neither a reference to safety performance indicators, so this matter should be subject of the next step detailed assessment / operating license request. It should be noted, however, that some collection of data is envisaged as the design includes consideration of anticipated transients (art. 4.35).

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

The use of Operating Experience in the design has been documented. The process is also supported by the various programmes of the Westinghouse Owners Group.

4.62–4.65 Documentation

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

Review Results

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

The 'UK AP1000 Safety, Security, and Environmental Report' is structured in the standard DCD format following the guidance on contents and format given in Regulatory Guide 1.70, Revision 3, 'Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants - LWR Edition', November 1978. Where appropriate, the DCD is subdivided beyond the extent of the standard format to provide additional information specifically required for that area. Similarly, some of the passive features of the AP1000 require modification of the standard format and content either in terms of placement or type of material presented (1.1.6.1_r1).

The information provided in the DCD strictly follows US NRC standard procedures. The level of detail of the DCD goes beyond the present UK HSE Step 2 request. Due to the well-known standard format it provided easy reference to support statements made in the Head Document. The Safety analyses are presented in Chapter 15 in a transparent way, including the initial conditions, computer codes used, nominal values of plant characteristics used in the analyses and uncertainties, set points of safety system actuation and time delays, plant systems and equipment available for transient and accident conditions, single failures assumed and non –safety equipment used for accident mitigation (15-0_r1.). For each accident the code used in the analysis is characterized and the main assumptions for the accident are given, then the scenario is described, the results are presented and discussed and the conclusions are formulated. Radiological aspects include determination of source terms, definition of methodology used in radiation hazard calculations and results. App.15a presents evaluation models and parameters for analysis of radiological consequences of accidents, and App.15b the removal of airborne activity from the containment atmosphere following a LOCA. Further analyses performed within the study of PSA are presented in Vol. 3 of DCD and include all external and internal events up to severe accidents, determining their frequencies, related source terms and doses to the population.

Emphasis is given to provide information on how various safety criteria and requirements are addressed. Compliance with US NRC Regulatory Criteria including 'Three Mile Island Issues' and the list of 'Unresolved Safety Issues and Generic Issues' is systematically

addressed in DCD Chapter 1.9. The AP1000 has undergone the US NRC design certification process. The NRC Final Safety Evaluation Report for AP1000 Design is appended as Section F of the documentation. It is stated that there are no open items. Document 1 Section C 'Safety Assessment Roadmap for AP1000 Design' provides information on how the results of safety analyses described in the DCD and the PRA, aimed at demonstrating compliance with the NRC criteria, address the SAPs of the UK HSE. Document 1 Section D 'Western European Nuclear Regulators' Association Roadmap' provides a description on how the design complies with the WENRA safety reference levels. It is stated that the design meets the WENRA requirements. Section B of Document 1 summarizes information on how the design addresses the US Advanced Light Water Reactor Utility Requirements (URD) and the European Utility Requirements (EUR).

The IAEA Draft Requirement 4.57 requests the establishment of criteria for judging safety by the designer, the operating organization (once it has been established) and the regulatory body. Based on the assessments of the various criteria referred to above, the Requesting Party concludes "that the AP1000 design has addressed all relevant UK Safety Assessment Principles in sufficient detail". Regarding numerical targets and legal limits it is indicated that "the AP1000 standard design meets these limits, supports the Duty Holder in meeting the limits, or is anticipated to meet the limits." It is noticed that some further analysis may be required when site-specific information is known.

The review showed several areas where the US approach does not explicitly address Requirements of the IAEA Safety Standards or the UK HSE SAPs. These include e.g. categorisation of events/accidents, classification of safety functions/systems, accident consequence calculations, use of SAMDA assessments, and issues related to PSA. These areas need to be reviewed in more detail at the next step.

Also areas have been identified where additional information would need to be provided to support the claims made. In particular these include more details related to the functioning of the passive and simplified safety systems (emergency core cooling and decay heat removal), the scaling of these systems from experimental size to the AP 600 and then to the AP1000, mitigation of severe accidents by melt arrest within the RPV, containment protection in case in-vessel melt arrest is not successful, PSA related issues including the use of results from the AP 600 PSA, increased burnup, extended plant life, uncertainty analyses related to core layout, stability analysis, and validation of computer codes. These areas would need to be reviewed in more detail at the next step.

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

Review Results

The Requirement is addressed. Both quantitative and qualitative outcomes of the safety assessment are presented (DCD Vol. 1 Sections A, B, C, D). The evidence of robustness and reliability of the safety assessment and its assumptions is presented in Vol. 2 Chapter 15 dealing with the safety analyses. The information on the performance of individual systems is presented in Chapters 3-10 of DCD Vol. 2. Possible failures of individual safety related system components are considered in DCD Vol. 3 and not only for design basis accidents, but also for severe accident conditions (Vol. 3 App. D)

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

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

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

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

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

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

Review Results

The Requirement is addressed. The document includes anticipated operational occurrences and accident conditions according to the US NRC Reg. Guide 1.70, and in addition those scenarios which involve failures of passive safety systems included in AP1000 design. The review of US NRC confirmed that the list of AOO s and accidents considered in SAR content of SAR is complete and larger than required by RG 1.70.

An overview of the data is provided in Vol. 2 Chapter 1, together with uncertainties and the way of modeling. Computer codes used and assumptions made are included in the descriptions of accident scenarios in Volumes 2 and 3 for deterministic and probabilistic analyses, respectively.

The criteria used for the evaluation of modeling results are given in Chapter 1.2.1.

The results of the analyses including performance of plant systems, incurred risks and discussion of uncertainties are given in Vol. 2 Chapter 15 for deterministic and in Vol. 3 for probabilistic analyses. The latter include frequencies of severe accidents, radioactive releases, and estimates of doses to the population at various distances from the plant and for various time lengths.

Conclusions on the acceptability of the level of safety achieved are presented in DCD Vol. 1 sections A, B, C, and D. A discussion of possible additional measures is given in the App. 1B_r1 on SAMDA evaluation.