

Table of Contents

[1.0 Introduction 3](#_Toc499293292)

[2.0 Highlights of the Results and Conclusions 9](#_Toc499293293)

[3.0 References 11](#_Toc499293294)

[4.0 Acronyms 13](#_Toc499293295)

[5.0 Applications of Key IAEA Definitions to the AP1000 Plant Design 15](#_Toc499293296)

[6.0 AP1000 Plant Design Compliance Assessment 21](#_Toc499293297)

**Trademarks:**

**AP1000** is a trademark or registered trademark of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited.

Inconel is a trademark or registered trademark of its owner. Other names may be trademarks of their respective owners.

1.0 Introduction

The International Atomic Energy Agency (IAEA) safety standards establish fundamental safety principles, requirements and measures to control the radiation exposure of people and the release of radioactive material to the environment, to restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation, and to mitigate the consequences of such events if they were to occur. The standards apply to facilities and activities that give rise to radiation risks, including nuclear installations, the use of radiation and radioactive sources, the transport of radioactive material and the management of radioactive waste.

The IAEA safety standards reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from harmful effects of ionizing radiation. The issues in the IAEA Safety Standards Series are divided into three categories:

1. **Safety Fundamentals** – present the fundamental safety objectives and principles of protection and safety, and provide the basis for the safety requirements
2. **Safety Requirements** – establish the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements are governed by the objectives and principles of the Safety Fundamentals.
3. **Safety Guides –** provide recommendations and guidance on how to comply with the safety requirements, indicating an international consensus that it is necessary to take the measures recommended (or equivalent alternative measures). The Safety Guides present international good practices, and increasingly they reflect best practices, to help users striving to achieve high levels of safety. The recommendations provided in the Safety Guides are expressed as “should” statements.

IAEA Safety Standard No. SSR-2/1 includes the following sections and requirements:

INTRODUCTION

APPLYING THE SAFETY PRINCIPLES AND CONCEPTS

MANAGEMENT OF SAFETY IN DESIGN

Requirement 1: Responsibilities in the management of safety in plant design

Requirement 2: Management system for plant design

Requirement 3: Safety of the plant design throughout the lifetime of the plant

PRINCIPAL TECHNICAL REQUIREMENTS

Requirement 4: Fundamental safety functions

Requirement 5: Radiation protection in design

Requirement 6: Design for a nuclear power plant

Requirement 7: Application of defence in depth

Requirement 8: Interfaces of safety with security and safeguards

Requirement 9: Proven engineering practices

Requirement 10: Safety assessment

Requirement 11: Provision for construction

Requirement 12: Features to facilitate radioactive waste management and decommissioning

GENERAL PLANT DESIGN

Requirement 13: Categories of plant states

Requirement 14: Design basis for items important to safety

Requirement 15: Design limits

Requirement 16: Postulated initiating events

Requirement 17: Internal and external hazards

Requirement 18: Engineering design rules

Requirement 19: Design basis accidents

Requirement 20: Design extension conditions

Requirement 21: Physical separation and independence of safety systems

Requirement 22: Safety classification

Requirement 23: Reliability of items important to safety

Requirement 24: Common cause failures

Requirement 25: Single failure criterion

Requirement 26: Fail-safe design

Requirement 27: Support service systems

Requirement 28: Operational limits and conditions for safe operation

Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety

Requirement 30: Qualification of items important to safety

Requirement 31: Ageing management

Requirement 32: Design for optimal operator performance

Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant

Requirement 34: Systems containing fissile material or radioactive material

Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination

Requirement 36: Escape routes from the plant

Requirement 37: Communication systems at the plant

Requirement 38: Control of access to the plant

Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety

Requirement 40: Prevention of harmful interactions of systems important to safety

Requirement 41: Interactions between the electrical power grid and the plant

Requirement 42: Safety analysis of the plant design

DESIGN OF SPECIFIC PLANT SYSTEMS

Reactor core and associated features

Requirement 43: Performance of fuel elements and assemblies

Requirement 44: Structural capability of the reactor core

Requirement 45: Control of the reactor core

Requirement 46: Reactor shutdown

Requirement 47: Design of reactor coolant systems

Requirement 48: Overpressure protection of the reactor coolant pressure boundary

Requirement 49: Inventory of reactor coolant

Requirement 50: Cleanup of reactor coolant

Requirement 51: Removal of residual heat from the reactor core

Requirement 52: Emergency cooling of the reactor core

Requirement 53: Heat transfer to an ultimate heat sink

Requirement 54: Containment system for the reactor

Requirement 55: Control of radioactive releases from the containment

Requirement 56: Isolation of the containment

Requirement 57: Access to the containment

Requirement 58: Control of containment conditions

Requirement 59: Provision of instrumentation

Requirement 60: Control systems

Requirement 61: Protection system

Requirement 62: Reliability and testability of instrumentation and control systems

Requirement 63: Use of computer based equipment in systems important to safety

Requirement 64: Separation of protection systems and control systems

Requirement 65: Control room

Requirement 66: Supplementary control room

Requirement 67: Emergency response facilities on the site

Requirement 68: Design for withstanding the loss of off-site power

Requirement 69: Performance of supporting systems and auxiliary systems

Requirement 70: Heat transport systems

Requirement 71: Process sampling systems and post-accident sampling systems

Requirement 72: Compressed air systems

Requirement 73: Air conditioning systems and ventilation systems

Requirement 74: Fire protection systems

Requirement 75: Lighting systems

Requirement 76: Overhead lifting equipment

Requirement 77: Steam supply system, feedwater system and turbine generators

Requirement 78: Systems for treatment and control of waste

Requirement 79: Systems for treatment and control of effluents

Requirement 80: Fuel handling and storage systems

Requirement 81: Design for radiation protection

Requirement 82: Means of radiation monitoring

The purpose of this report is to asssess the **AP1000®** plant design against the IAEA Safety Standard No. SSR-2/1 Rev. 1 [1], which was published in 2016 and incorporates the lessons learned from the Fukushima event.

The **AP1000** plant is an 1100-MWe pressurized water reactor (PWR) with passive safety features and extensive plant simplifications that enhance construction, operation, maintenance and safety. One of the key design approaches in the **AP1000** plant is to use passive features to mitigate design basis accidents (DBAs). In addition to redundancy, these features incorporate diversity based on probabilistic risk assessment (PRA, also called Probabilistic Safety Assessment or PSA) insights. Active defense-in-depth (DiD) features provide investment protection, reduce the demands on the passive features and support the aggressive PSA targets. The passive features are classified as safety in the United States (US). The active DiD features are classified as **AP1000** Plant Class D, e.g. as non-safety (with supplemental requirements) in the US. The **AP1000** plant Class D corresponds to lower tier safety classes in European classification scheme (UK safety class 2, European Utility Requirements [EUR] F2 functions) and meets the relevant design and quality assurance requirements. See also Section 5.0 for a more detailed discussion of safety classification.

The **AP1000** plant has incorporated a standardization approach, which together with the level of safety achieved by the passive safety features, results in a plant design that can be applied to different geographical regions with varying regulatory standards and utility expectations without major changes.

The **AP1000** plant is designed to achieve a high safety and performance record. It is conservatively based on proven PWR technology, but with an emphasis on safety features that rely on natural forces. Consistent with current practice, DiD systems are used as the first level of defense against more probable events. As the second level of defense, the **AP1000** plant uses passive safety systems to further enhance plant safety and to satisfy utility requirements (e.g., EUR, Electric Power Research Institute [EPRI] Utility Requirements Document [URD]). Safety systems use natural driving forces such as pressurized gas, gravity flow, natural circulation flow, and convection. Safety systems do not use active components (such as pumps, fans or diesel generators) and are designed to function without safety-grade support systems (such as alternating current [ac] power; component cooling water; service water; heating, ventilating and air conditioning [HVAC]). The number and complexity of operator actions required to control the safety systems are minimized; the approach is to eliminate operator action rather than automate it.

The **AP1000** plant is designed to meet United States Nuclear Regulatory Commission (US NRC) deterministic safety criteria and probabilistic safety criteria with large margins. Safety analyses have been completed and documented in the US licensing documents reviewed by the US NRC (the **AP1000** plant Design Control Document [DCD] [2] and PRA [4]). The extensive **AP600** plant testing program, which is applicable to the **AP1000** plant design, verifies that the innovative plant features will perform as designed and analyzed. PRA results show a very low core damage and large release frequency, which meet the goals established for advanced reactor designs. The core damage frequency, considering internal, fire and flood events during at-power and shutdown operation is about 5E‑7/yr. The large release frequency for these same events is about 6E-8/yr. This very low risk was a result of the **AP1000** plant safety design features (simple passive safety features and active DiD features) as well as the use of PRA throughout the design process starting with the initial design phase. In addition, the **AP1000** plant has carefully evaluated and addressed severe accident phenomenon; a key **AP1000** plant designfeature in dealing with a severe accident is the in-vessel retention of a molten core. This feature provides a robust, reliable, and simple means of preventing a molten core from causing containment failure.

The **AP1000** plant is a standardized plant design that uses conservative, bounding site parameters (temperatures, wind velocities and seismic levels), achieves a very high level of safety and incorporates utility operational desires. As a result, it is a plant design that can be applied to different geographical regions around the world with varying regulatory standards and utility expectations without major changes.

The **AP1000** plant design provides adequate protection of the public health and safety with respect to aircraft impact. Following an aircraft impact, the **AP1000** plant is capable of maintaining adequate core cooling, containment integrity, spent fuel pool integrity, and spent fuel cooling.

A complete list of references utilized to perform the assessment are provided in Section 3.0 of this report, while Section 4.0 provides a complete list of the acronyms and trademarks used throughout the document. Key IAEA definitions are applied to the AP1000 design plant in Section 5.0 in support of the paragraph by paragraph compliance assessment presented in Section 6.0.

2.0 Highlights of the Results and Conclusions

The **AP1000** plant passive design represents a significant improvement over conventional PWRs and is developed around the fundamental design principles of safety, simplification and standardization. The development of the **AP1000** plant safety concept based on passive systems allows full realization of the benefits of these fundamental design principles. The adoption of passive systems as the primary means to deliver safety functions, combined with reliable DiD active systems, achieves both an un-paralleled level of safety and optimized support for investment protection. The active DiD systems are effective in minimizing the demand on the passive systems for more frequent postulated faults, thus ensuring stable and continued production of electricity.

The results of assessment show that the **AP1000** plant design fully meets the intent of IAEA Standard No. SSR-2/1 Rev. 1 in regards to safety of nuclear power plants.

The **AP1000** plant design has also been extensively reviewed:

* The EUR compliance was awarded to the **AP1000** plant design in May 2007.
* Under the new US licensing approach, Westinghouse has first submitted the AP600 design in 1992 for certification to the US NRC which granted Final Design Approval in 1999. The **AP1000** plant design was submitted in 2002 and certified by the US NRC in January 2006. In May 2007, Westinghouse submitted an application to amend the **AP1000** certified plant design to resolve several issues that would otherwise be left to combined operating license applicants and to enhance security and aircraft crash resistance. The **AP1000** plant final design certification was granted by the US NRC in December 2011. In total the combined US NRC review of the Westinghouse advance passive technology represents an effort of 206 man-years [3].
* The US NRC issued combined operating license to allow Southern Nuclear Operating Company and South Carolina Electric & Gas Company to construct and operate **AP1000** plants at the existing Vogtle and VC Summer sites in Georgia and South Carolina, respectively.
* In China preliminary safety analysis reports were submitted for the Sanmen and Haiyang **AP1000** plant projects to the National Nuclear Safety Administration (NNSA) in 2008. Following its review, NNSA has issue all construction permits in 2009 for both sites. The final safety analysis reports for both sites were submitted to NNSA in 2012.
* In support to commercial activities in Canada, Westinghouse requested that Phase 1 and Phase 2 pre-licensing reviews of the **AP1000** plant design be carried out by the Canadian Nuclear Safety Commission. The review was completed in June 2013. The Canadian Nuclear Safety Commission concluded that there are no fundamental barriers to licensing the **AP1000** plant design in Canada.
* In December 2011 the United Kingdom (UK) regulators granted Interim Design Acceptance Confirmation and Interim Statement of Design Acceptability to the AP1000 plant design following four and a half years of work as part of the Generic Design Assessment (GDA) of the **AP1000** plant. The **AP1000** plant GDA restarted in 2015 and concluded in March 2017 with the issuance of a Design Acceptance Confirmation and Statement of Design Acceptability.

3.0 References

[1] IAEA Safety Standards Series No. SSR-2/1 (Rev. 1). Safety of Nuclear Power Plants: Design. International Atomic Energy Agency, Vienna, 2016.

[2] APP-GW-GL-700, Rev.19. AP1000 Design Control Document.

[3] Gorgemans, J., Corletti, M.M., Delong, R.A. and Schulz, T.L. (2014). Learning through Delivery, Westinghouse AP1000® Plant Licensing. Proceedings of the 22th International Conference on Nuclear Engineering ICONE22, July 7-11, 2014, Prague, Czech Republic. (Archived in PRIME as WAAP-8786, Rev. 1)

[4] APP-GW-GL-022, Rev. 8. AP1000 Probabilistic Risk Assessment.

[5] WCAP-16675-P (Proprietary) and WCAP-16675-NP (Non-Proprietary), Rev. 8. AP1000 Protection and Safety Monitoring System Architecture Technical Report.

[6] UKP-GW-GL-790, Rev. 7. UK AP1000 Environment Report.

[7] NDA Technical Note no. 11339711, Geological Disposal Generic Design Assessment: Summary of Disposability Assessment for Wastes and Spent Fuel arising from Operation of the Westinghouse AP1000.

*Available online:* <http://www.westinghousenuclear.com/Portals/5/Documents/documentation%20pdfs/Generic%20Design%20Assessment%20-%20Summary%20of%20Disposability%20Assessment%20for%20Wastes%20and%20Spent%20Fuel%20arising%20from%20Operation%20of%20the%20Westinghouse%20AP1000.pdf>

[8] APP-GW-GL-058, Rev. 0. Assessment of AP1000 Compliance with IAEA Safety Standards, Safety Fundamentals No. SF-1, Vienna 2006.

[9] EPS-GW-GSR-001, Rev. 0. AP1000 Compliance Analysis with EUR Target for Plant Condition 4 – DBA.

[10] EPS-GW-GSR-002, Rev. 0. AP1000 Compliance Analysis with EUR Target for DEC.

[11] WCAP-15800, Rev. 3. Operational Assessment for AP1000.

[12] APP-GW-GL-100, Rev. 0. AP1000 Conformance with Nuclear Regulatory Commission General Design Criteria.

[13] Not used.

[14] NPP\_NPP\_000065, Rev. 0. Westinghouse **AP1000** Nuclear Power Plant – Coping with Station Blackout.

[15] NPP\_NPP\_000067, Rev. 0. Westinghouse **AP1000** Nuclear Power Plant – Spent Fuel Pool Cooling).

[16] NPP\_NPP\_000072, Rev. 0. Westinghouse **AP1000** Nuclear Power Plant – Response to External Hazards.

[17] EPS-GW-GL-701, Rev. C. **AP1000** Plant Evaluation of Western European Nuclear Regulators’ Association Safety Objectives for New Power Reactors.

[18] WCAP-15992, Rev. 1, AP1000 Adverse Systems Interactions Evaluation Report.

[19] UKP-GW-GL-793, Rev. 1. AP1000 Pre-Construction Safety Report.

[20] IAEA Safety Glossary, Terminology Used In Nuclear Safety And Radiation Protection, 2016 Revision.

*Available online: <http://www-ns.iaea.org/downloads/standards/glossary/iaea-safety-glossary-rev2016.pdf>*

[21] American National Standards Institute N18.2, Nuclear Safety Criteria for the Design of Stationary PWR Plants, 1973.

[22] WCAP-1599, Rev. 2, Evaluation of the AP1000 Conformance to Inter-System Loss-of-Coolant Accident Acceptance Criteria.

4.0 Acronyms

|  |  |
| --- | --- |
| ac Alternating Current  ALARA As Low As Reasonably Achievable  ANSI American National Standards Institute  ASME American Society of Mechanical Engineers  ATWS Anticipated Transient Without Scram  BTP Branch Technology Position  CFR Code of Federal Regulations  CVS Chemical and Volume Control System  DAS Diverse Actuation System  DBA Design Basis Accident  DBE Design Basis Event  DCD Design Control Document  DEC Design Extension Condition  DiD Defense-in-Depth  D-RAP Design Reliability Assurance Program  EPRI Electric Power Research Institute  EUR European Utility Requirements  GDA Generic Design Assessment  GDC General Design Criteria  HVAC Heating, Ventilating and Air Conditioning  I&C Instrumentation and Control  IAEA International Atomic Energy Agency  IDS Class 1E dc and Uninterruptable Power Supply System  IEEE Institute of Electrical and Electronic Engineers  LOCA Loss of Coolant Accident  MCR Main Control Room  NFPA National Fire Protection Association  NNSA National Nuclear Safety Administration  PLS Plant Control System |  |

PMS Protection and Safety Monitoring System

PRA Probabilistic Risk Assessment

PSA Probabilistic Safety Assessment

PWR Pressurized Water Reactor

QMS Quality Management System

RCS Reactor Coolant System

RMS Radiation Monitoring System

SSC System, Structure and Components

UK United Kingdom

URD Utility Requirements Document

US United States

US NRC United States Nuclear Regulatory Commission

WENRA Western European Nuclear Regulators’ Association

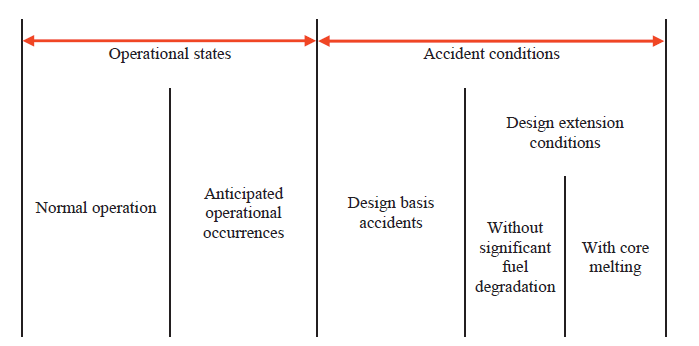
5.0 Applications of Key IAEA Definitions to the AP1000 Plant Design

In this section, key definitions from [1] and from [20] are discussed and applied to the **AP1000** plant design to suppot the interpretation of the IAEA requirements in Section 6.0.

Plant States

The IAEA defines the plant states as follows in [1].

**Plant states** (considered in design).



**Figure 1 Plant States (from [1])**

**Accident conditions**. Deviations from normal operation that are less frequent and more severe than anticipated operational occurrences (AOOs).

* Accident conditions comprise DBAs and design extension conditions (DECs).

**DBA.** A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.

**DEC.** Postulated accident conditions that are not considered for DBAs, but that are considered in the design process for the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. DEC comprise conditions in events without significant fuel degradation and conditions in events with core melting.

As detailed in Chapter 15 of the **AP1000** plant DCD [2], the plant states considered in the **AP1000** plant design were defined based on the American National Standards Institute (ANSI) 18.2 [21] classification which divides plant conditions into four categories according to anticipated frequency of occurrence and potential radiological consequences to the public. The four categories are as follows:

* Condition I: Normal operation and operational transients, which corresponds to the normal operation defined by the IAEA.
* Condition II: Faults of moderate frequency, which broadly corresponds to the AOOs defined by the IAEA.
* Condition III: Infrequent faults, which belong to the DBAs as defined by the IAEA.
* Condition IV: Limiting faults, which belong to the DBAs as defined by the IAEA.

The basic principle applied in relating design requirements to each of the conditions is that the most probable occurrences should yield the least radiological risk, and those extreme situations having the potential for the greatest risk should be those least likely to occur.

Additional accident sequences are considered in the **AP1000** plant design:

* Non-core melt multiple failure sequences are considered in the analysis of anticipated transients without scram (ATWS). An ATWS is an AOO during which an automatic reactor scram is required but fails to occur due to a common mode fault in the reactor protection system. The analysis is described in Section 15.8 of the **AP1000** plant DCD [2].
* Additional non-core melt mutliple failure sequences are considered in the **AP1000** plant Level 1 PRA success criteria analyses described in [4] and in Chapter 19 of the **AP1000** plant DCD [2].
* Core melt sequences are analyzed in the **AP1000** plant Level 2 PRA analyses described in [4] and in Chapter 19 of the **AP1000** plant DCD [2], including the evaluation of the severe accident phenomena and fission product source terms, as well as the modeling of the containment event tree and associated success criteria.

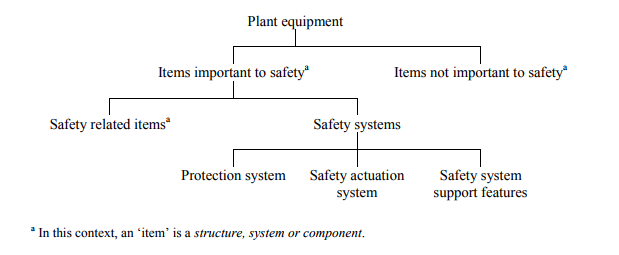
Safety Classification

The **AP1000** plant safety classification presented in Section 3.2.2 of the **AP1000** plant DCD [2] has been developed to meet the requirements set out in various US regulations. The following definitions are used in standard **AP1000** plant documentation:

* **Safety-related** is a classification applied to items relied upon to remain functional during or following a design basis event (DBE, i.e. an AOO or a DBA) to provide a safety-related function.
* **Safety-related function** is a function that is relied upon during or following a DBE to provide for the following:
  + The integrity of the reactor coolant pressure boundary
  + The capability to shut down the reactor and maintain it in a safe shutdown condition
  + The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guideline exposures of 10 Code of Federal Regulations (CFR) 50.34.
* **Defense-in-Depth (DiD)**: In the **AP1000** plant design, DiD is used to indicate certain structures, systems and components (SSCs) that, while not safety-related, do provide additional means of performing key safety functions and thus provide additional DiD to the passive safety-related features. The DiD SSCs are typically active systems whose operation relies on ac power.
* **Severe Accident Mitigation Features**: The **AP1000** plant design includes several features to minimize the potential for large fission product releases and for monitoring and controlling hydrogen inside the containment in the event of a severe accident. These features are aimed at both the prevention and mitigation of severe accident phenomena that can threaten containment integrity. Equipment used to mitigate the effects of severe accidents is not treated in the same manner as safety-related equipment because of the low likelihood of a severe accident to occur. However, equipment used to mitigate severe accidents is designed to survive the environmental conditions identified in the **AP1000** plant PRA evaluation to provide reasonable assurance that the equipment will operate in the severe accident environment for which they are intended and over the time span for which they are needed.
* **Non-Safety-Related**: Any SSC that does not meet the criteria of safety-related or DiD but which may still contribute to maintaining nuclear safety.

However, a different set of definitions are used by the IAEA. The following paragraphs apply the IAEA definitions to the **AP1000** plant.

The IAEA safety glossary [20] provides the following classification of the plant equipment:



**Figure 2 IAEA Classification of Plant Equipment (from [20])**

* **Item important to safety**. An item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public. Items important to safety include:
  + Those SSCs whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;
  + Those SSCs that prevent AOOs from leading to accident conditions;
  + Those features that are provided to mitigate the consequences of malfunction or failure of structures, systems and components.

For the **AP1000** plant, the items important to safety, as defined per the IAEA, englobe the safety-related and the DiD SSCs, as well as the severe accident mitigation features.

* **Safety system**. A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the reactor core, or to limit the consequences of AOOs and DBAs. Safety systems consist of the protection system, the safety actuation systems and the safety system support features.

The safety systems, as defined per the IAEA, are thus those qualified as “safety-related” in the **AP1000** plant safety classification.

* **Protection system**. System that monitors the operation of a reactor and which, on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition.

For the **AP1000** plant, the protection and safety montoring system (PMS) fulfills these functions.

* **Safety system settings**. Settings for levels at which safety systems are automatically actuated in the event of AOOs or DBAs, to prevent safety limits from being exceeded.

For the **AP1000** plant, the safety system settings, or actuation setpoints, are described in Sections 7.2 and 7.3 of the **AP1000** plant DCD [2].

* **Safety actuation system**. The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system.

For the **AP1000** plant, the safety actuation system, as defined per the IAEA, englobes all the passive safety systems.

* **Safety system support features**. The collection of equipment that provides services such as cooling, lubrication and energy supply required by the protection system and the safety actuation systems.

For the **AP1000 plant**, the only safety system support feature, as defined per the IAEA, is the Class 1E dc and Uninterruptable Power Supply System (IDS).

* **Safety related system**. A system important to safety that is not part of a safety system.

For the **AP1000** plant,the safety related systems, as defined per the IAEA, are thus the **AP1000** plant DiD SSCs and the severe accident mitigation features.

6.0 AP1000 Plant Design Compliance Assessment

This section provides the detailed assessment of the **AP1000** plant design against IAEA Safety Standard No. SSR-2/1 – Safety of Nuclear Power Plants: Design.

| **Section or Para.** | **Sub-Para.** | **Safety Requirements No. SSR 2/1Text**  **Note: The references noted in [ ] in this column do not relate to the reference list in Section 3.0 of this document but relate to the reference list of the IAEA Safety Standard No. SSR-2/1.** | | **AP1000 Plant Design Information** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **1.0** |  | **INTRODUCTION** | |  | | |
|  |  | **BACKGROUND** | |  | | |
| 1.1 | 1 | The present publication supersedes the Safety Requirements publication Safety of Nuclear Power Plants: Design,1 which was issued in 2012 as IAEA Safety Standards Series No. SSR-2/1. Account has been taken of the Fundamental Safety Principles [1], published in 2006. Requirements for nuclear safety are intended to ensure “the highest standards of safety that can reasonably be achieved” for the protection of workers, the public and the environment from harmful effects of ionizing radiation arising from nuclear power plants and other nuclear facilities. It is recognized that technology and scientific knowledge advance, and that nuclear safety and the adequacy of protection against radiation risks need to be considered in the context of the present state of knowledge. Safety requirements will change over time; this Safety Requirements publication reflects the present consensus.  *Footnote: 1 INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards* *Series No. SSR-2/1, IAEA, Vienna (2012).* | | This is an explanatory statement. | | |
| 1.2 | 1 | The designs of many existing nuclear power plants, as well as the designs for new nuclear power plants, have been enhanced to include additional measures to mitigate the consequences of complex accident sequences involving multiple failures and of severe accidents. Complementary systems and equipment with new capabilities have been backfitted to many existing nuclear power plants to aid in the prevention of severe accidents and the mitigation of their consequences. Guidance on the mitigation of severe accidents has been provided at most existing nuclear power plants. The design of new nuclear power plants now explicitly includes the consideration of severe accident scenarios and strategies for their management. Requirements related to the State system of accounting for, and control of, nuclear material and security related requirements are also taken into account in the design of nuclear power plants. Integration of safety measures and security measures will help to ensure that neither compromise the other. | | This is an explanatory statement. | | |
| 1.3 | 1 | It might not be practicable to apply all the requirements of this Safety Requirements publication to nuclear power plants that are already in operation or under construction. In addition, it might not be feasible to modify designs that have already been approved by regulatory bodies. For the safety analysis of such designs, it is expected that a comparison will be made with the current standards, for example as part of the periodic safety review for the plant, to determine whether the safe operation of the plant could be further enhanced by means of reasonably practicable safety improvements. | | This is an explanatory statement. | | |
|  |  | **OBJECTIVE** | |  | | |
| 1.4 | 1 | This publication establishes design requirements for the structures, systems and components of a nuclear power plant, as well as for procedures and organizational processes important to safety that are required to be met for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events, were they to occur. | | This is an explanatory statement. | | |
| 1.5 | 1 | This publication is intended for use by organizations involved in design, manufacture, construction, modification, maintenance, operation and decommissioning for nuclear power plants, in analysis, verification and review and in the provision of technical support, as well as by regulatory bodies. | | This is an explanatory statement. | | |
|  |  | **SCOPE** | |  | | |
| 1.6 | 1 | It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). This publication may be applied, with judgement, to other reactor types, to determine the requirements that have to be considered in developing the design. | | This is an explanatory statement. | | |
| 1.7 | 1 | This publication does not address:  (a) Requirements that are specifically covered in other IAEA Safety Requirements publications (e.g. IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), Safety Assessment for Facilities and Activities [2]);  (b) Matters relating to nuclear security or to the State system of accounting for, and control of, nuclear material;  (c) Conventional industrial safety that under no circumstances could affect the safety of the nuclear power plant;  (d) Non-radiological impacts arising from the operation of nuclear power plants. | | This is an explanatory statement. | | |
| 1.8 | 1 | Terms in this publication are to be understood as defined and explained in the IAEA Safety Glossary [3], unless otherwise stated here (see Definitions). | | This is an explanatory statement. | | |
|  |  | **STRUCTURE** | |  | | |
| 1.9 | 1 | This Safety Requirements publication follows the relationship between safety objectives and safety principles, and between requirements for nuclear safety functions and design criteria for safety. Section 2 elaborates on the safety objective, safety principles and concepts that form the basis for deriving the safety function requirements that must be met for the nuclear power plant, as well as the safety design criteria. Sections 3-6 establish numbered overarching requirements (shown in bold type), with additional requirements as appropriate in the paragraphs that follow them. Section 3 establishes the general requirements to be satisfied by the design organization in the management of safety in the design process. Section 4 establishes requirements for the principal technical design criteria for safety, including requirements for the fundamental safety functions, the application of defence in depth and provisions for construction; requirements for interfaces of safety with nuclear security and with the State system of accounting for, and control of, nuclear material; and requirements for ensuring that radiation risks arising from the plant are maintained as low as reasonably achievable. Section 5 establishes requirements for general plant design that supplement the requirements for principal technical design criteria to ensure that safety objectives are met and the safety principles are applied. | | This is an explanatory statement. | | |
| 1.9 | 1  (cont.) | The requirements for general plant design apply to all items (i.e., structures, systems and components) important to safety. Section 6 establishes the requirements for the design of specific plant systems, such as the reactor core, reactor coolant systems, containment system, and instrumentation and control systems. | | This is an explanatory statement. | | |
| **2.0** |  | **APPLYING THE SAFETY OBJECTIVE, SAFETY PRINCIPLES AND CONCEPTS** | |  | | |
| 2.1 | 1 | The Fundamental Safety Principles [1] establish one fundamental safety objective and ten safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and for the safety of facilities and activities that give rise to radiation risks. | | This is an explanatory statement. Refer to “Assessment of **AP1000** plant design compliance with IAEA SF-1 Fundamental Safety Principles”, APP‑GW‑GL‑058 [8]. | | |
| 2.2 | 1 | This fundamental safety objective has to be achieved and the ten safety principles have to be applied, without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks. To ensure that nuclear power plants are operated and activities are conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken to achieve the following (see para. 2.1 of the Fundamental Safety Principles [1]):  (a) To control the radiation exposure of people and the release of radioactive material to the environment during operational states;  (b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source, spent nuclear fuel, radioactive waste or any other source of radiation at a nuclear power plant;  (c) To mitigate the consequences of such events if they were to occur. | | This is an explanatory statement. Refer to “Assessment of **AP1000** plant design compliance with IAEA SF-1 Fundamental Safety Principles”, APP‑GW‑GL‑058 [8]. | | |
| 2.3 | 1 | The fundamental safety objective applies for all stages in the lifetime of a nuclear power plant, including planning, siting, design, manufacture, construction, commissioning and operation, as well as decommissioning. This includes the associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste. (see para. 2.2 of the Fundamental Safety Principles [1]) | | This is an explanatory statement. Refer to “Assessment of **AP1000** plant design compliance with IAEA SF-1 Fundamental Safety Principles”, APP‑GW‑GL‑058 [8]. | | |
| 2.4 | 1 | Paragraph 2.3 of the Fundamental Safety Principles [1] states that: “Ten safety principles have been formulated, on the basis of which safety requirements are developed and safety measures are to be implemented in order to achieve the fundamental safety objective. The safety principles form a set that is applicable in its entirety; although in practice different principles may be more or less important in relation to particular circumstances, the appropriate application of all relevant principles is required.” | | This is an explanatory statement. Refer to “Assessment of **AP1000** plant design compliance with IAEA SF-1 Fundamental Safety Principles”, APP‑GW‑GL‑058 [8]. | | |
| 2.5 | 1 | This Safety Requirements publication establishes requirements that apply those safety principles, which are particularly important in the design of nuclear power plants. | | This is an explanatory statement. | | |
|  |  | **RADIATION PROTECTION IN DESIGN** | |  | | |
| 2.6 | 1 | In order to satisfy the safety principles, it is required to ensure that for all operational states of a nuclear power plant and for any associated activities, doses from exposure to radiation within the installation or exposure due to any planned radioactive release from the installation are kept below the dose limits and kept as low as reasonably achievable. In addition, it is required to take measures for mitigating the radiological consequences of any accidents, were they to occur. | | The effectiveness of the **AP1000** plant features that limit radiation releases and offsite doses are shown in the **AP1000** plant DCD [2] Chapters 11, 12 and 15 . On-site accident management procedures and off-site intervention measures (if any) are provided by the plant owner/operator.  Refer to the **AP1000** plant DCD [2] Chapter 12 for the principles for assuring that occupational radiation exposure is as low as reasonably achievable (ALARA) and other radiation design features. Refer to Chapters 15 and 19 for deterministic and probabilistic releases and dose assessments.  Note that two sets of radiological consequence analyses have been performed for the **AP1000** plant design. In the US, radiological consequences have historically been calculated using very conservative methodologies (where consideration of severe accidents is included as part of the design basis dose analyses), and likewise compared with specific acceptance criteria consistent with those conservative assumptions. The dose analyses presented in Chapter 15 of the **AP1000** plant DCD [2] were performed in this content. For UK licensing, dose calculations were performed using more realistic assumptions, consistent with common regulatory practice outside of the US. These are described in Chapters 9 and 10 of the **AP1000** plant Pre-Construction Safety Report (PCSR, [19]). | | |
| 2.7 | 1 | To apply the safety principles, it is also required that nuclear power plants be designed and operated so as to keep all sources of radiation under strict technical and administrative control. However, this principle does not preclude limited exposures or the release of authorized amounts of radioactive substances to the environment from nuclear power plants in operational states. Such exposures and radioactive releases are required to be strictly controlled and to be kept as low as reasonably achievable, in compliance with regulatory and operational limits as well as radiation protection requirements [4]. | | The **AP1000** plant is designed to keep all sources of radiation under control. Refer to the **AP1000** plant DCD [2] Chapters 11 and 12 for discussion of sources, releases, and measures to keep exposures ALARA and within regulatory limits.  The **AP1000** plant DCD [2] Section 11.3.3 discusses doses at the site boundary due to activity released as a result of normal operations. | | |
|  |  | **SAFETY IN DESIGN** | |  | | |
| 2.8 | 1 | To achieve the highest level of safety that can reasonably be achieved in the design of a nuclear power plant, measures are required to be taken to do the following, consistent with national acceptance criteria and safety objectives [1]:  (a) To prevent accidents with harmful consequences resulting from a loss of control over the reactor core or other sources of radiation, and to mitigate the consequences of accidents that do occur;  (b) To ensure that for all accidents taken into account in the design of the installation, any radiological consequences would be below the relevant limits and would be kept as low as reasonably achievable;  (c) To ensure that the likelihood of occurrence of an accident with serious radiological consequences is extremely low and that the radiological consequences of such an accident would be mitigated to the fullest extent practicable. | | The **AP1000** plant design has been developed to provide such measures:   1. Many design measures prevent potential accidents with harmful consequences (for example, ensuring that piping stresses are limited and comply with leak-before-break piping design criteria and sealless reactor coolant pumps). Refer to the **AP1000** plant DCD [2] Section 1.2 for general description of plant features. The passive safety systems provide highly effective mitigation of accidents. Refer to the **AP1000** plant DCD [2] Chapters 6, 15 and 19 for further details. 2. The **AP1000** plant DCD [2] Chapter 15 provides the deterministic safety analysis of DBAs to show that relevant dose limits are met. The **AP1000** plant DCD [2] Chapter 1 Appendix 1B provides an assessment of additional design measures not included in the **AP1000** plant design, showing these additional measures would not significantly reduce radiological consequences. 3. The **AP1000** plant DCD [2] Chapter 19 provides the PRA showing the extremely low likelihood of serious radiological consequences and that mitigation measures are effective for severe accidents. | | |
| 2.9 | 1 | To demonstrate that the fundamental safety objective [1] is achieved in the design of a nuclear power plant, a comprehensive safety assessment [2] of the design is required to be carried out. Its objective is to identify all possible sources of radiation and to evaluate possible doses that could be received by workers at the installation and by members of the public, as well as the possible effects on the environment, as a result of operation of the plant. The safety assessment is required in order to examine: (i) normal operation of the plant; (ii) the performance of the plant in anticipated operational occurrences; and (iii) accident conditions. On the basis of this analysis, the capability of the design to withstand postulated initiating events and accidents can be established, the effectiveness of the items important to safety can be demonstrated, and the inputs (prerequisites) for emergency planning can be established. | | The **AP1000** plant DCD [2] as a whole provides such a comprehensive safety assessment. Chapter 15, in particular, provides the deterministic safety analysis of DBAs to show the capability of the design to withstand postulated initiating events.  The **AP1000** plant provides large safety margins and reduced safety risk by applying passive safety systems that rely on natural driving forces, such as gravity and convection.  The **AP1000** plant design is recognized internationally and has been reviewed by regulators around the world, including China, the UK, and Canada. The **AP1000** plant is the first Generation III+ reactor design to obtain final design approval and a construction and operating license from the US NRC. It also has received a design acceptance confirmation from the UK regulatory authorities as part of the GDA process. The **AP1000** plant design has been independently assessed and confirmed to meet the requirements of the EUR document and the EPRI URD. | | |
| 2.10 | 1 | Measures are required to be taken to control exposure for all operational states at levels that are as low as reasonably achievable and to minimize the likelihood of an accident that could lead to a loss of control over a source of radiation. Nevertheless, there will remain a possibility that an accident could happen. Measures are required to be taken to ensure that the radiological consequences of an accident would be mitigated. Such measures include the provision of safety features and safety systems, the establishment of accident management procedures by the operating organization and, possibly, the establishment of off-site protective actions by the appropriate authorities, supported as necessary by the operating organization, to mitigate exposures if an accident has occurred. | | The effectiveness of the **AP1000** plant features that limit radiation releases and offsite doses are shown in the **AP1000** plant DCD [2] Chapters 11, 12 and 15. On site accident management procedures and off site intervention measures (if any) are provided by the plant licensee.  Refer to the **AP1000** plant DCD [2] Chapter 12 for the principles for assuring that occupational radiation exposure is ALARA and other radiation design features. Refer to the **AP1000** plant DCD [2] Chapters 15 and 19 for deterministic and probabilistic releases and dose assessments, respectively. | | |
| 2.11 | 1 | The design for safety of a nuclear power plant applies the safety principle that practical measures must be taken to mitigate the consequences for human life and health and the environment of nuclear or radiation incidents (Principle 8 of the Fundamental Safety Principles [1]). Plant event sequences that could result in high radiation doses or large radioactive releases have to be practically eliminated2 and plant event sequences with a significant frequency of occurrence must have no, or only minor, potential radiological consequences. An essential objective is that the necessity for off-site protective actions to mitigate radiological consequences be limited or even eliminated in technical terms, although such measures might still be required by the responsible authorities.  *Footnote: 2 The possibility of certain conditions arising may be considered to have been ‘practically eliminated’ if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.* | | The **AP1000** plant PRA described in the **AP1000** plant DCD [2] Chapter 19 shows that severe accidents with large or early releases can be considered to have been practically eliminated by virtue of their extremely low frequency. The **AP1000** plant DCD [2] Chapter 1 Appendix 1B provides assessment of additional design measures not included in the **AP1000** plant design, showing these additional measures would not significantly reduce radiological consequences.  The accident analyses in the **AP1000** plant DCD [2] Chapter 15 demonstrate that radiation releases are small for more frequent events. Furthermore, the mitigation features are shown to prevent core uncovery following postulated Loss of Coolant Accidents (LOCAs) ≤8 inch (200 mm DN) equivalent pipe diameter in size; and that core peak clad temperature and cladding oxidation are limited and well below recognized limits.  Offsite intervention measures are decided on a site specific basis. The **AP1000** plant design goal for site boundary whole‑body dose and the acute red bone marrow dose is <25 rems (0.25 sieverts), at a frequency not to exceed 1x10-6 per year.  EPS-GW-GL-701 [17] discusses in more details the **AP1000** plant compliance with the objective of practical elimination of large and early release, as well as the limitations of off-site protective actions. | | |
|  |  | **THE CONCEPT OF DEFENCE IN DEPTH** | |  | | |
| 2.12 | 1 | The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth [1, 5, 6]. This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant. | | The **AP1000** plant DCD [2] as a whole shows that the concept of defense in depth is applied in the **AP1000** plant design.  EPS-GW-GL-701 [17] discusses in more details the **AP1000** plant compliance with the concept of defense in depth. | | |
| 2.13 | 1 | Paragraph 3.31 of the Fundamental Safety Principles [1] states that:  “Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available.... The independent effectiveness of the different levels of defence is a necessary element of defence in depth.” | | The **AP1000** plant design provides for multiple levels of defense for accident mitigation (defense-in-depth), resulting in extremely low core damage probabilities while minimizing the occurrences of containment flooding, pressurization, and heat-up. Defense-in-depth is integral to the **AP1000** plant design, with a multitude of individual plant features capable of providing some degree of defense of plant safety. The **AP1000** plant DCD [2] Chapter 1 discusses these levels of defense. | | |
| 2.13 (cont.) | 2-3 | There are five levels of defence:  (1) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction, and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices. | | The **first level of defense** is achieved in the **AP1000** plant 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. To enhance the first level of defense the Westinghouse Quality Management System (QMS) dictates the procedures to follow during the design/procurement/commissioning of the plant. (**AP1000** plant DCD [2] Section 17.3). | | |
| 2.13 (cont.) | 4-5 | (2) The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or else to minimize their consequences, and to return the plant to a safe state.  (3) For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. In the design of the plant such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be capable of preventing damage to the reactor core or preventing radioactive releases and returning the plant to a safe state. | | In normal operation, the **second level of defense** ensures that the plant can be operated stably and reliably. This is achieved by the Plant Control System (PLS) as discussed in the **AP1000** plant DCD [2] Section 7.1.3 and the active DiD systems. The active DiD systems are designed with redundancy for operational reliability, and mitigation of the more probable events. These reliable DiD systems automatically actuate to provide a first level of defense to reduce the likelihood of unnecessary actuation and operation of the passive safety systems for AOOs.  In the **third level of defense**, the PMS, as described in the **AP1000** plant DCD [2] Section 7.1.2, controls the deviations from normal operating conditions and automatically actuates the passive safety systems. It is an independent and highly reliable control system from the PLS. The PMS reliability is assessed in the **AP1000** plantPRA [4]. The **AP1000** plantpassive safety systems and equipment are sufficient to automatically establish and maintain core cooling and containment integrity for at least 72 hours following a DBE, assuming the most limiting single failure, with no operator action, and no on‑site or off-site ac power sources. Following the 72 hour period, simple actions can be taken by the operator to align further on-site cooling and power sources and extend the operation of the passive safety systems for another four days. | | |
| 2.13 (cont.) | 6 | (4) The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release3 are required to be ‘practically eliminated’4.  *Footnotes: 3 An ‘early radioactive release’ in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A ‘large radioactive release’ is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.*  *4 The possibility of certain conditions arising may be considered to have been ‘practically eliminated’ if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise* | | An additional level of defense is provided through diverse mitigation functions that are included within the passive safety systems. This **fourth level of defense** mitigates multiple failure events. Diversity exists, for example, in the residual heat removal function. The passive residual heat removal heat exchanger is the passive safety feature for removing core decay heat during a transient. In case of multiple failures that prevent the passive residual heat removal heat exchanger to function, another level of defense is provided by the passive safety injection functions of the Passive Core Cooling System (PXS) and automatic depressurization function of the Reactor Coolant System (RCS) via passive feed and bleed. The diverse actuation system (DAS) actuates the passive safety systems in case of PMS failure.  The **AP1000** plant design features enhanced safety such that no severe release of fission products is predicted to occur from an initially intact containment for several days after the onset of core damage, assuming no actions for recovery. This time enables accident management actions to mitigate the accident and prevent containment failure to be performed. The total plant frequency (which includes internal events, internal fire and internal flood events, at power and at shutdown) of large release as predicted by the PRA is 5.9E-8 events per reactor year, which is much lower than for currently operating plants. | | |
| 2.13 (cont.) | 6 |  | | The philosophy of the **AP1000** plant core melt accident mitigation is the in-vessel-retention of the damaged core, supported by passive containment cooling and adequate hydrogen management. The **AP1000** plantis designed to drain the high capacity in-containment refueling water storage tank water into the reactor cavity in the event that the core has overheated. This provides cooling on the outside of the reactor vessel preventing reactor vessel failure and subsequent spilling of molten core debris into the containment. Retention of debris in the vessel significantly reduces uncertainty in the assessment of containment failure and radioactive release to the environment as ex‑vessel severe accident phenomena such as the interaction of molten core material with concrete and ex-vessel steam explosion are precluded. Additional design provisions are included to prevent releases to the public: a large containment volume, hydrogen igniters, and passive autocatalytic recombiners. The **AP1000** plant design also includes controlled containment venting capability which is not credited in the PRA but which is part of the measures identified in the severe accident mitigation guidelines to prevent containment failure in case of a core melt accident and failure of the core melt mitigation measures. | | |
| 2.13 (cont.) | 6 |  | | The operation of the passive cooling system also limits the fission products in the containment atmosphere. Effective passive aerosol deposition occurs within the **AP1000** plant containment primarily by gravitational sedimentation and by thermophoresis and diffusiophoresis removal mechanisms promoted by the heat transfer to the containment cooling surface. As a defense-in-depth measure, the **AP1000** plant containment design includes an active containment spray feature. The containment spray strategy is outlined in the severe accident mitigation guidelines. In the event of a loss of containment integrity as indicted by high radiation levels detected outside containment, the containment spray system may be activated to wash aerosol fission products from the containment atmosphere to reduce the releases to the environment. | | |
| 2.13 (cont.) | 7 | (5) The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accident conditions. This requires the provision of an adequately equipped emergency control centre, and emergency plans and emergency procedures for on-site and off-site emergency response. | | For the **fifth level of defense**, the **AP1000** plant main control room and remote shutdown workstation each provide capability to control and monitor key plant functions. The **AP1000** plant design also provides a control support area in the annex building that can be utilized as a technical support center if a licensee chooses. The off-site emergency control centers are out of scope of the standard design since they are site specific. Their location and design will be addressed by the site licensee.  The effectiveness of the **AP1000** plant features that limit radiation releases and offsite doses are shown in the **AP1000** plant DCD [2] Chapters 11, 12, 15 and 19. On site accident management procedures and off site intervention measures (if any) are provided by the plant licensee. However, Westinghouse provides a standard set of AP1000 plant procedures using recognized good industry practice that can be used by the Operator to define site specific procedures. These procedures include the following: abnormal operating procedures, emergency operating procedures, and severe accident management guidelines. Severe accident mitigation guidelines for instance provide guidance to the operators and emergency response personnel on how to respond to a plant emergency where specific plant parameters have reached a point where core damage may have occurred. | | |
| 2.13 (cont.) | 1-7 |  | | EPS-GW-GL-701 [17] discusses in more details the **AP1000** plant compliance with the concept of defence in depth, as well as with the objective of practical elimination of large and early release. | | |
| 2.14 | 1 | A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherently safe features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term in terms of amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures. | | The **AP1000** plant provides defense-in-depth barriers as described in the **AP1000** plant DCD [2] Section 3.1.2.  One of the most recognizable aspects of defense-in-depth is the protection of public safety through the physical plant boundaries. Releases of radiation from the reactor core are prevented by the fuel cladding, the reactor pressure boundary, and the containment pressure boundary. As described in response to 2.13, the AP1000 plant defense –in-depth relies on both active and passive systems. Inherent design features also support the protection of the physical plant barriers: “When the reactor is critical, the negative fuel temperature reactivity effects (Doppler feedback) provide prompt reactivity feedback to compensate for a rapid, uncontrolled reactivity excursion. The negative Doppler coefficient of reactivity is provided by the use of a low-enrichment fuel design. This Doppler feedback is the primary reactivity feedback mechanism to provide the inherent core reactivity protection during rapid core reactivity excursions. For slower reactivity transients that result in moderator temperature increases, the nonpositive moderator temperature coefficient of reactivity provides compensatory reactivity feedback to help control these slower transients. The overall core design establishes a nonpositive moderator temperature coefficient of reactivity.”  Releases of radiation from the spent fuel stored in the auxiliary building are prevented by the fuel cladding, the spent fuel pool, and the ventilation systems serving the radiologically controlled area of the auxiliary building. | | |
|  |  | **MAINTAINING THE INTEGRITY OF DESIGN OF THE PLANT THROUGHOUT THE LIFETIME OF THE PLANT** | |  | | |
| 2.15 | 1 | The design, construction and commissioning of a nuclear power plant might be shared between a number of organizations: the architect-engineer, the vendor of the reactor and its supporting systems; the suppliers of major components; the designers of electrical systems; and the suppliers of other systems that are important to the safety of the plant. | | This is an explanatory statement. | | |
| 2.16 | 1 | The prime responsibility for safety rests with the person or organization responsible for facilities and activities that give rise to radiation risks (i.e., the operating organization) [1]. In 2003, the International Nuclear Safety Advisory Group suggested that the operating organization could set up a formal process to maintain the integrity of design of the plant throughout the lifetime of the plant (i.e. during the operating lifetime and into the decommissioning stage). A formally designated entity within the operating organization would take responsibility for this process. | | The plant licensee is responsible for establishing the plant configuration management program. The **AP1000** plant design configuration management program used by Westinghouse provides input for the owner/operator program. The **AP1000** plant design basis documentation supports the plant licensee program. | | |
| 2.17 | 1 | In practice, the design of a nuclear power plant is complete only when the full plant specification (including site details) is produced for its procurement and licensing. Reference [7] emphasizes the need for a formally designated entity that has overall responsibility for the design process and is responsible for approving design changes and for ensuring that the requisite knowledge is maintained. Reference [7] also introduces the concept of ‘responsible designers’ to whom this formally designated entity could assign specific responsibilities for the design of parts of the plant. Prior to an application for authorization of a plant, the responsibility for the design will rest with the design organization (e.g. the vendor). Once an application for authorization of a plant has been made, the prime responsibility for safety will lie with the applicant; although detailed knowledge of the design will rest with the responsible designers. This balance will change as the plant is put into operation, since much of this detailed knowledge, such as the knowledge embodied in the safety analysis report, design manuals and other design documentation, will be transferred to the operating organization. To facilitate this transfer of knowledge, the structure of the formally designated entity that has overall responsibility for the design process would be established at an early stage. | | Such transition of design responsibility from the design organization to the operating organization is designated as part of **AP1000** plant project implementation plans. | | |
| 2.18 | 1 | The management system requirements that are placed on the formally designated entity would also apply to the responsible designers. However, the overall responsibility for maintaining the integrity of design of the plant would rest with the formally designated entity, and hence ultimately with the operating organization. | | The **AP1000** plant design is regulated by the Westinghouse QMS program through its procedures, which apply to every aspect of the nuclear power plant design, procurement, commissioning and turn over to the operating entity. (see the **AP1000** plant DCD [2] Section 17.3)  Such transition of design responsibility from the design organization to the operating organization is designated as part of **AP1000** plant project implementation plans. | | |
| **3.0** |  | **MANAGEMENT OF SAFETY IN DESIGN** | |  | | |
|  |  | **Requirement 1: Responsibilities in the management of safety in plant design**  **An applicant for a license to construct and/or operate a nuclear power plant shall be responsible for ensuring that the design submitted to the regulatory body meets all applicable safety requirements.** | | The **AP1000** plant DCD [2] is the base document for demonstrating that the standard **AP1000** plant design meets applicable safety requirements in the US. The owner/operator as applicant for a license to construct and/or operate an **AP1000** plant in the US takes responsibility for applying the **AP1000** plant DCD [2] information together with site and owner specific information to ensure the design submitted meets applicable safety requirements.  Adaptation of the licensing process in other countries is designated as part of **AP1000** plant project implementation plans. | | |
| 3.1 | 1 | All organizations, including the design organization5, engaged in activities important to the safety of the design of a nuclear power plant shall be responsible for ensuring that safety matters are given the highest priority.  *Footnote: 5**The design organization is the organization responsible for preparation of the final detailed design of the plant to be built.* | | The Westinghouse QMS and associated procedures give safety matters the highest priority. Refer to the **AP1000** plant DCD [2] Section 17.3. | | |
|  |  | **Requirement 2: Management system** **for plant design**  **The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design.** | | The Westinghouse QMS (and its predecessors) provides the mechanisms for ensuring the safety requirements are met in the **AP1000** plant design. Refer to the **AP1000** plant DCD [2] Section 17.3. The **AP1000** plant DCD [2] provides documentation for the safety requirements, and Chapter 14 specifies inspections, tests, and analyses required to be performed to demonstrate the plant is constructed in accordance with the DCD requirements. | | |
| 3.2 | 1 | The management system6 shall include provision for ensuring the quality of design of each structure, system and component, as well as the overall design of the nuclear power plant, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes.  *Footnote: 6 Requirements on the management system are established in IAEA Safety Standards Series No. GS-R-3, The Management System for Facilities and Activities [8].* | | The Westinghouse QMS and associated procedures provide the mechanisms to ensure quality of the **AP1000** plant design, for identification and correction of design deficiencies, for checking the adequacy of the design and for controlling design changes. Refer to the **AP1000** plant DCD [2] Section 17.3. | | |
| 3.3 | 1 | The design of the plant, including subsequent changes, modifications or safety improvements, shall be in accordance with established procedures that call on appropriate engineering codes and standards and shall incorporate relevant requirements and design bases. Interfaces shall be identified and controlled. | | The Westinghouse QMS and associated procedures are applied in the **AP1000** plant design for this purpose. | | |
| 3.4 | 1 | The adequacy of the plant design, including design tools and design inputs and outputs, shall be verified and validated by individuals or groups separate from those who originally performed the design work. Verification, validation and approval of the plant design shall be completed as soon as is practicable in the design and construction process, and in any case before operation of the plant is commenced. | | The Westinghouse QMS and associated procedures provide the mechanisms for verification and validation of the **AP1000** plant design.  For example, according to the Westinghouse QMS periodic Design Reviews are performed. Operators/owners, Westinghouse experts and independent Industry experts participate in the design reviews. The Design Review process is a step in verifying and validating design aspects. Furthermore it allows a steady and continuous information flow between the plant designer and the owner/operator. | | |
|  |  | **Requirement 3: Safety of the plant design throughout the lifetime of the plant**  **The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.** | | This is a requirement of the plant owner/operator. The plant designer serves as a resource to the owner/operator over the plant life. | | |
| 3.5 | 1 | The formal system for ensuring the continuing safety of the plant design shall include a formally designated entity responsible for the safety of the plant design within the operating organization’s management system. Tasks that are assigned to external organizations (referred to as responsible designers) for the design of specific parts of the plant shall be taken into account in the arrangements. | | This is a requirement of the plant owner/operator. The plant designer serves as a resource to the owner/operator over the plant life. | | |
| 3.6 | 1-4 | The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure the following:  (a) That the plant design is fit for purpose and meets the requirement for the optimization of protection and safety by keeping radiation risks as low as reasonably achievable;  (b) That the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design;  (c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings; | | (a) See response for Paragraphs 2.6, 2.7, 2.10 and Requirements 5, 12, and 78.  (b) The results of the safety analyses as detailed in the **AP1000** plant DCD [2] Chapter 6, Section 9.1, and Chapter 15 and the PRA in the **AP1000** plant DCD [2] Chapter 19 provide evidence that the capability of the safety SSCs, and procedures to control and limit the consequences of failures and deviations from normal operation thus ensuring the design is robust. The final ownership and responsibility for plant procedures resides with the Plant Operator. However, Westinghouse provides a standard set of **AP1000** plant procedures for operating, emergency, abnormal, maintenance, and test activities using recognized good industry practice that can be used by the Operator to define site specific procedures. (see response for Paragraph 4.11).  (c) Westinghouse provides a standard set of **AP1000** plant procedures for operating, emergency, abnormal, maintenance, and test activities using recognized good industry practice that can be used by the Operator to define site specific procedures. (see response to Requirement 4.11). The **AP1000** plant DCD [2] Section 16.1 provides the Technical Specifications, e.g. a dynamic set of plant parameters, associated limits and conditions for plant operation, and associated SSCs, that provide the delivery of safety functions. Short term availability controls are also defined for the active DiD systems (the **AP1000** plant DCD [2] Section 16.3). | | |
| 3.6 (cont.) | 5-9 | (d) That management of design requirements and configuration control are maintained;  (e) That the necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled;  (f) That the necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization;  (g) That all design changes to the plant are reviewed, verified, documented and approved;  (h) That adequate documentation is maintained to facilitate future decommissioning of the plant. | | (d) See response for Requirement 2.  (e) The Westinghouse QMS and associated procedures provide the means to ensure quality of the **AP1000** plant design and for the management of suppliers. Refer to the **AP1000** plant DCD [2] Section 17.3.  (f) This is a requirement of the plant owner/operator. The plant designer serves as a resource to the owner/operator over the plant life.  (g) See response for Paragraph 3.4.  (h) The Westinghouse QMS and associated procedures provide the mechanisms to ensure quality of the **AP1000** plant design, for identification and correction of design deficiencies, for checking the adequacy of the design and for controlling design changes. Refer to the **AP1000** plant DCD [2] Section 17.3. | | |
| **4.0** |  | **PRINCIPAL TECHNICAL REQUIREMENTS** | |  | | |
|  |  | **Requirement 4: Fundamental safety functions**  **Fulfillment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity, (ii) removal of heat from the reactor and from the fuel store and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.** | | These requirements are met by the **AP1000** plant as presented in the **AP1000** plant DCD Chapter 15 for the DBAs and in the **AP1000** plant DCD [2] Chapter 19 and the **AP1000** plant PRA [4] for DECs. Spent fuel decay heat removal is discussed in the **AP1000** plant DCD [2] Section 9.1.3, and containment heat removal is discussed in the **AP1000** plant DCD [2] Chapter 6. Shielding and control of releases are discussed in the **AP1000** plant DCD [2] Chapters 11 and 12. | | |
| 4.1 | 1 | A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the fundamental safety functions and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states. | | The **AP1000** plant safety analyses (**AP1000** plant DCD [2] Chapter 6, Section 9.1, and Chapter 15) and the associated Technical Specifications (**AP1000** plant DCD [2], Section 16.1) identify and confirm the SSCs required to fulfill safety functions in response to each initiating event. The **AP1000** plant DCD [2] Chapter 19 Appendix 19E provides a systematic evaluation of events that could occur during shutdown conditions.  Additionally, beside the deterministic safety analyses, the PRA quantifies plant response to a spectrum of initiating events to demonstrate the low probability of core damage and resultant risk to the public. PRA input includes specific values for the reliability of the various SSCs in the plant that are used to respond to postulated initiating events. The Design Reliability Assurance Program (D-RAP) - see **AP1000** plant DCD [2] Section 17.4) is implemented as an integral part of the design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the PRA will remain valid throughout plant life. The Operational Phase Reliability Assurance Activities provides confidence that the operations and maintenance activities performed by the operating plant should maintain the reliability assumptions made in the plant PRA.  The **AP1000** plant DCD [2] Section 16.1 provides the plant Technical Specifications, e.g. a dynamic set of plant parameters, associated limits and conditions for plant operation, and associated SSCs, that provide the delivery of safety functions for the **AP1000** plant. | | |
| 4.2 | 1 | Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled. | | The **AP1000** plant safety display information is used by the operator to monitor and maintain the safety of the plant throughout operating conditions that include AOOs and accident and post-accident conditions. Refer to the **AP1000** plant DCD [2] Section 7.5 | | |
|  |  | **Requirement 5: Radiation protection**  **The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits; that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following accident conditions.** | | The **AP1000** plant design has been developed to minimize the risk of exposing people and the environment to harmful radiation. Provisions and design aspects for maintaining personnel exposures ALARA throughout the plant lifetime are presented in the **AP1000** plant DCD [2] Chapter 12. Dose evaluations for the **AP1000** plant are presented in the **AP1000** plant DCD [2] and 12 (worker doses and public doses at the site boundary for normal operations) and in the **AP1000** plant DCD [2] Chapter 15 (doses from accidents). The **AP1000** plant Section 11.5 describes how the radiation monitoring system supports the ALARA design goal.  The basic management philosophy guiding the **AP1000** plant design so that radiation exposures are ALARA include:   * Design SSCs for reliability and maintainability, thereby effectively reducing the maintenance requirements on radioactive components. * Design SSCs to reduce the radiation fields, thereby allowing operation, maintenance and inspection activities to be performed in the minimum design radiation field. * Design SSCs to reduce access, repair and removal times, thereby effectively reducing the time spent in radiation fields during operation, maintenance, and inspection. | | |
|  |  | **Requirement 5: Radiation protection (cont.)** | | * Design SSCs to accommodate remote and semi-remote operation, maintenance and inspection, thereby effectively reducing the time spent in radiation fields.   **AP1000** plant design features to promote ALARA are described in the **AP1000** plant DCD [2] Section 12.3. Examples of features that assist in maintaining exposures ALARA in the **AP1000** plant include:   * Provision of features to allow maintenance of state-of-the-art reactor coolant chemistry conditions, such that corrosion and consequential source terms are minimized: these include pH control capability sufficient to meet current and evolving industry standards and the ability to add zinc to the primary coolant. * Provision of features to allow draining, flushing, and decontaminating equipment and piping. * Design of equipment to minimize the creation and buildup of radioactive material and to ease flushing of crud traps. * Provision of shielding for personnel protection during maintenance or repairs and during decommissioning. * Provision of means and adequate space for the use of movable shielding. * Separation of more highly radioactive equipment from less radioactive equipment and provision of separate shielded compartments for adjacent items of radioactive equipment. * Provision of shielded access hatches for installation and removal of plant components. | | |
|  |  | **Requirement 5: Radiation protection (cont.)** | | * Provision of design features, such as the chemical and volume control system (CVS), to minimize crud buildup. * Provision for means and adequate space for the use of remote and robotic maintenance and inspection equipment. * Simplifying the plant design compared to previous PWRs with design approaches such as:   + Elimination of boron recycle;   + Elimination of evaporators;   + Use of an extended fuel cycle;   + Reduction in components containing radioactive fluids. * Clearly and deliberately separating clean areas from potentially radioactive ones. | | |
| 4.3 | 1 | The design shall be such as to ensure that plant states that could lead to high radiation doses or large radioactive releases are practically eliminated7, and that there are no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence.  *Footnote: 7 The possibility of certain conditions arising may be considered to have been ‘practically eliminated’ if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.* | | The radiation dose criteria used for the **AP1000** plant are described in the **AP1000** plant DCD [2] Chapter 15 and follow this concept that more frequent events have limits that result in very low consequences, and only low frequency events have limits, based on very conservative assumptions, at the high end of acceptability. The **AP1000** plant PRA described in the **AP1000** plant DCD [2] Chapter 19 shows that severe accidents with large or early releases can be considered to have been practically eliminated by virtue of their extremely low frequency of occurrence. | | |
| 4.4 | 1 | Acceptable limits for purposes of radiation protection8 associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.  *Footnote: 8 Requirements on radiation protection and safety of radiation sources are established in IAEA Safety Standards Series No. GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [9*]. | | In accordance with US regulations the radiation dose criteria used is described in the **AP1000** plant DCD [2] Chapter 15 and is associated with categories of plant states. Assessment of the **AP1000** plant design against the US radiological limits has been performed and shown to be acceptable (see the **AP1000** plant DCD [2] Chapter 15). In addition, the **AP1000** plant design has been assessed against the radiological dose criteria as defined in the EUR to ensure design requirements are met. These analyses are document in References [9] and [10]. | | |
|  |  | **Requirement 6: Design for a nuclear power plant**  **The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.** | | The **AP1000** plant has been developed based on extensive use of deterministic and probabilistic analyses to determine that radiation risks arising throughout the plant lifecycle ALARA . See **AP1000** plant DCD [2] Chapters 15 and 19. As evidenced by the safety analyses results (the **AP1000** plant DCD [2] Chapter 6, Section 9.1, and Chapter 15) and the low probabilities of core damage and significant releases determined by the PRA (**AP1000** plant DCD [2] Chapter 19): the **AP1000** plant and items important to safety have the capability to perform their safety functions with the necessary reliability.  The **AP1000** plant DCD [2] Section 16.1 provides the **AP1000** plant Technical Specifications, e.g. a dynamic set of plant parameters, associated limits and conditions for plant operation, and associated SSCs, that provide the delivery of safety functions for the **AP1000** plant.  Environmental impact assessments have been performed for an **AP1000** plant at several sites in the US and in China, with acceptable results. Radiation exposure to the environment is minimized by virtue of reducing waste streams to the extent practical (see **AP1000** plant DCD [2] Chapter 11). The impact on the environment due to decommissioning of the **AP1000** plant is discussed in **AP100**0 plant Environment Report (ER) [6] developed in support to the UK GDA. | | |
| 4.5 | 1 | The design for a nuclear power plant shall be such as to ensure that the safety requirements of the operating organization, the requirements of the regulatory body and the requirements of relevant legislation, as well as applicable national and international codes and standards, are all met, and that due account is taken of human capabilities and human limitations and of factors that could influence human performance. Adequate information on the design shall be provided for ensuring the safe operation and the maintenance of the plant, and to allow subsequent plant modifications to be made. Recommended practices shall be provided for incorporation into the administrative and operational procedures for the plant (i.e. the operational limits and conditions). | | The **AP1000** plant “Plant Life Cycle Safety Report,” (UKP-GW-GL-737, Rev. 2, “[PLCSR]), developed in support of the **AP1000** plant GDA in the UK, provides guidance on verifying the construction process and performance of initial tests, analyses, and acceptance criteria to demonstrate that these requirements are satisfied on a project specific basis.  The **AP1000** plant DCD [2] in general specifies the safety requirements (of the operating organization, regulatory body, legislation, codes and standards) and how the design addresses these requirements as part of project implementation. The **AP1000** plant DCD [2] Chapter 18 discusses the **AP1000** plant human factors engineering program. **AP1000** plant information provided to the operating organization is sufficient for that organization to assume its role and responsibility for safe and efficient plant operation. The **AP1000** plant DCD [2] Chapter 16 provides the basis for the operating organization’s operational limits and conditions.  The **AP1000** plant design is recognized internationally and has been reviewed by regulators around the world, including China, the UK, and Canada. The **AP1000** PWR has obtained final design approval from the US NRC and design acceptability confirmation from UK regulatory authorities as part of the GDA process. The **AP1000** plant has been licensed for construction in the US and has received an operating license, as well as construction approval in China. The **AP1000** plant design has been independently assessed and confirmed to meet the requirements of the EUR document and the EPRI URD. | | |
| 4.6 | 1 | The design shall take due account of relevant available experience that has been gained in the design, construction and operation of other nuclear power plants, and of the results of relevant research programmes. | | The **AP1000** plant has taken into account previous operational experience as discussed in the **AP1000** plant DCD [2] Sections 1.2 (URD) and 1.9, and WCAP-15800 “Operational Assessment for AP1000” [10].  The **AP1000** plant design has been independently assessed and confirmed to meet the requirements of the EUR document and the EPRI URD which address utility requirements for the next generation of nuclear reactors.  With each new **AP1000** plant constructed, **AP1000** plant standardization has allowed lessons learned to be swiftly and efficiently applied to future new **AP1000** plant projects.  Also see response for Paragraph 3.3. | | |
| 4.7 | 1 | The design shall take due account of the results of deterministic safety analyses and probabilistic safety analyses, to ensure that due consideration is given to the prevention of accidents and to mitigation of the consequences of any accidents that do occur. | | The **AP1000** plant design balances the prevention of accidents and their mitigation in the case they occur.  Refer to the response to Requirements 1, 2, 3. The DiD systems provide investment protection actuating as one of the first lines of defense for mitigation of an abnormal condition and minimize the demand on the passive safety systems. If DiD systems are not sufficient to recover from the event the passive safety systems will actuate. Diversity incorporated into the passive safety systems based on the PRA insights, allow them to provide diverse passive means of mitigation of the most frequent occurrences.  The **AP1000** plant DCD [2] as a whole provides a comprehensive **AP1000** plant safety assessment. The deterministic safety analyses are discussed in the **AP1000** plant DCD [2] Chapter 6, Section 9.1, and Chapter 15; and the PRA are discussed in the **AP1000** plant DCD [2] Chapter 19. | | |
| 4.8 | 1 | The design shall be such as to ensure that the generation of radioactive waste and discharges are kept to the minimum practicable levels in terms of both activity and volume, by means of appropriate design measures and operational and decommissioning practices. | | The **AP1000** plant minimizes the activity and volume of radioactive waste as discussed in the **AP1000** plant DCD [2] Chapter 11. Waste minimization and decommissioning waste are also discussed in the **AP1000** plant ER [6] developed for the UK GDA. | | |
|  |  | **Requirement 7: Application of defence in depth**  **The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.** | | The independence between the Safety Systems is stated in US NRC General Design Criteria (GDC) 5, 22 and 24. **AP1000** plant designcompliance with the GDC criterion is discussed and documented in APP-GW-GL-100, “**AP1000** Conformance with US NRC General Design Criteria” [12].  The **AP1000** plant provides for multiple levels of defense with a high degree of independence, as demonstrated by safety assessments in the **AP1000** plant DCD [2] Chapters 15 and 19.  Also see response for Paragraph 2.13 and EPS-GW-GL-701, **AP1000** Evaluation of Western European Nuclear Regulators’ Association (WENRA) Safety Objectives for New Power Reactors [17] regarding compliance of the **AP1000** plant design to WENRA Safety Objective O4 (Independence between all levels of Defence-in-Depth). | | |
| 4.9 | 1 | The defence in depth concept shall be applied to provide several levels of defence that are aimed at preventing consequences of accidents that could lead to harmful effects on people and the environment, and ensuring that appropriate measures are taken for protection of people and the environment and for the mitigation of consequences in the event that prevention fails. | | Refer to the response for Paragraph 2.13 and Requirement 7. | | |
| 4.10 | 1 | The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times, and any relaxations shall be justified for specific modes of operation. | | The operation of the **AP1000** plant must be within the requirements of the operating equipment and plant conditions as stated in the Technical Specifications as presented in the **AP1000** plant DCD [2] Chapter 16. The Technical Specifications define the limiting conditions for operation, including requirements on the engineered safety functions. The plant operator is responsible for maintaining the Technical Specifications for Operation. The example Technical Specifications bases as presented in the **AP1000** plant DCD [2] Chapter 16 provides the justification for the selection of the Technical Specifications of Operation and any relaxation on the levels of defense available in the various operational modes.  In addition to the Technical Specifications which apply to the safety systems, the **AP1000** plant provides operational availability controls for the active DiD features as shown in the **AP1000** plant DCD [2] Section 16.3. | | |
| 4.11 | 1 | The design:  (a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;  (b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect9;  *Footnote: 9 A ‘cliff edge effect’, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.* | | Refer to the response for Paragraph 2.13 and Requirement 7. The **AP1000** plant design provides multiple levels of defense for accident mitigation, resulting in extremely low core damage probabilities. Defense-in-depth is integral to the **AP1000** plant design, with a multitude of individual plant features capable of providing some degree of defense of plant safety.  (a) **Physical plant Boundaries** - One of the most recognizable aspects of defense-in-depth is the protection of public safety through the physical plant boundaries. Releases of radiation are prevented by the fuel cladding, the reactor coolant pressure boundary, and the containment pressure boundary. See the **AP1000** plant DCD [2] Sections 1.1, 1.2 and 1.9. The **AP1000** plant DCD [2] Chapter 15 shows that core cooling and containment integrity capability for up to 72 hours following a DBE, assuming the most limiting single failure, no operator action, and no on-site and off-site ac power.  (b) The **AP1000** plant design and construction meets this requirement. In normal operation, the most fundamental level of defense-in-depth ensures that the plant can be operated stably and reliably. This is 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. See the **AP1000** plant DCD [2] Sections 1.1 and 1.2 for general design. Also see the **AP1000** plant DCD [2] Chapter 3 for design of SSCs. | | |
| 4.11 (cont.) | 4-5 | (c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible;  (d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized; | | (c) The instrumentation and control (I&C) architecture of the **AP1000** plant is presented in the **AP1000** plant DCD [2] Chapter 7. The PLS provides control during normal operations and transients. As presented in the **AP1000** plant DCD [2] Chapter 17, the **AP1000** plant D-RAP is implemented as an integral part of the **AP1000** plant design process to provide confidence that reliability is designed into the plant and that the important reliability assumptions made as part of the **AP1000** plant PRA will remain valid throughout plant life. The PRA quantifies plant response to a spectrum of initiating events to demonstrate the low probability of core damage and resultant risk to the public. For more probable events, the reliable active DiD systems automatically actuate to provide a first level of defense to reduce the likelihood of unnecessary actuation and operation of the safety passive systems. In addition, the engineered safety features are presented in the **AP1000** plant DCD [2] Chapter 6.  (d) The **AP1000** plant safety passive systems and equipment are sufficient to automatically establish and maintain core cooling and containment integrity for 72 hours following a DBE, assuming the most limiting single failure, no operator action, and no on-site and off-site ac power sources; the PMS actuates these systems. See the **AP1000** plant DCD [2] Chapter 6. | | |
| 4.11 (cont.) | 6 | (e) Shall provide for systems, structures and components and procedures to control the course of and, as far as is practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems; | | (e) The results of the safety analyses in the AP1000 plant DCD [2] Chapter 6, Section 9.1, and Chapter 15 and the PRA in the AP1000 plant DCD [2] Chapter 19 are evidence that the capability of the AP1000 plant safety SSCs and procedures to control the course of and as far as is practicable to limit the consequences of failures and deviations from normal operation is robust. The final ownership and responsibility for plant procedures resides with the Operator. However, Westinghouse provides a standard set of AP1000 plant procedures for operating, emergency, abnormal, maintenance, and test activities using recognized good industry practice that can be used by the Operator to define site specific procedures. These procedures include the following: normal operating procedures, abnormal operating procedures, emergency operating procedures, surveillance test procedures, maintenance procedures, alarm recovery procedures, severe accident management guidelines. | | |
| 4.11 (cont.) | 7 | (f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation. | | (f) An additional level of defense is provided through the diverse mitigation functions within the passive safety systems. This diversity exists, for example, in the residual heat removal function. The passive residual heat removal heat exchanger is the passive safety feature for removing decay heat during a transient. In case of multiple failures that prevent passive residual heat removal function, DiD is provided by the passive safety injection functions of the passive core cooling system and automatic depressurization function of the RCS (passive feed and bleed). See the **AP1000** plant DCD [2] Chapter 6.  The next level of defense-in‑depth is the availability of certain systems for reducing the potential for events leading to core damage. The **AP1000** plant design provides the operators with the ability to drain the in-containment refueling water storage tank water into the reactor cavity in the event that the core has uncovered and is melting. This prevents reactor vessel failure and subsequent relocation of molten core debris into the containment. Retention of the debris in the vessel provides for a high confidence that containment failure and radioactive release to the environment will not occur due to ex‑vessel severe accident phenomena.  The total plant frequency (which includes internal events, internal fire, internal flood, and shutdown hazards) of severe release as predicted by PRA is 5.9E-8 events per reactor year, which is much lower than for conventional plants. | | |
| 4.12 | 1 | To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable:  (a) Challenges to the integrity of physical barriers;  (b) Failure of one or more barriers;  (c) Failure of a barrier as a consequence of a failure of another barrier;  (d) The possibility of harmful consequences of errors in operation and maintenance. | | See response for Paragraph 4.11.   1. The **AP1000** plant design for stable, normal operation prevents challenges to the integrity of the physical barriers. In addition, the materials used to provide physical barriers have been shown to have a low probability of failure. Refer also to the discussion of the **AP1000** plant compliance with US NRC GDCs 14. 16, 30, 31 [12]. 2. & (c) The accident analyses presented in the **AP1000** plant DCD [2] Chapter 15 demonstrate how failure of a barrier is prevented when challenged, by the failure of another barrier or another event. Refer also to the discussion of the **AP1000** plant compliance with US NRC GDCs 14. 16, 30, 31 [12]. An additional level of defense for failure of a barrier as consequence of another barrier is provided through the diverse mitigation functions within the passive safety systems. Containment integrity is further protected by the next level of defense-in-depth, i.e. the availability of certain systems for reducing the potential for events leading to core damage. Severe accident mitigation guidelines provide guidance to the operators and emergency response personnel on how to respond to a plant emergency where specific plant parameters have reached a point where core damage may have occurred. | | |
| 4.12 (cont.) | 1 |  | | (c cont.)  The **AP1000** plant design provides the operators with the ability to drain the in-containment refueling water storage tank water into the reactor cavity in the event that the core has uncovered and is melting. This prevents reactor vessel failure and subsequent relocation of molten core debris into the containment. Retention of the debris in the vessel provides for a high confidence that containment failure and radioactive release to the environment will not occur due to ex-vessel severe accident phenomena. Analysis also shows there is a high confidence of a low probability of failure of the containment vessel if passive containment water cooling is maintained for 3 days and only air cooling is assumed afterwards.  (d) The **AP1000** plant DCD [2] Chapter 18 [2] describes the application of the human factors engineering disciplines to the design of the **AP1000** plant. | | |
| 4.13 | 1 | The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant. | | Refer to response for Paragraph 4.11 and Requirement 7. | | |
| 4.13A | 1 | The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems. | | Refer to response for Paragraph 4.11 and Requirement 7. See also EPS-GW-GL-701, **AP1000** Evaluation of Western European Nuclear Regulators’ Association (WENRA) Safety Objectives for New Power Reactors [17] regarding compliance of the **AP1000** plant design to WENRA Safety Objective O4 (Independence between all levels of Defence-in-Depth). | | |
|  |  | **Requirement 8: Interfaces of safety with security and safeguards**  **Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.** | | The **AP1000** plant safety and security measures have been developed in an integrated manner with active participation by utility organizations with plant operating experience. | | |
|  |  | **Requirement 9: Proven engineering practices**  **Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.** | | Industrial Codes and Standards are obtained and used in the **AP1000** plant design from the following organizations. Section 3.2 of the **AP1000** plant DCD [2] list the main codes and standards used in the design. Specific application of industrial codes and standards is provided in various sections of the **AP1000** plant DCD [2]. In addition to the internal verification the **AP1000** plant design has been reviewed by various safety authorities, such as the US NRC, the UK ONR and the Chinese NNSA. | | |
| 4.14 | 1 | Items important to safety for a nuclear power plant shall preferably be of a design that has previously been proven in equivalent applications, and if not, shall be items of high quality and of a technology that has been qualified and tested. | | The **AP1000** plant design is largely based on experience in the design and operation of existing plants. The power producing primary system is a familiar one based on proven and reliable Westinghouse PWR features, but with evolutionary improvements to be expected with the benefit of decades of operating experience, development of improved materials and better manufacturing techniques. For example, replacing Alloy 600 steam generator tubing with Alloy 690 tubing and the use of low cobalt-content alloys to reduce activation are some examples. This, of course, is a direct outgrowth of the steam generator replacements on the operating plants. A comparison of the major **AP1000** plant design features and nominal parameters with a typical two‑loop Westinghouse plant is provided in the **AP1000** plant DCD [2] Section 1.3.  Where applicable research and development program results obtained for the **AP600** configuration have been used to design the **AP1000** plant. This applies to materials, modular configuration of the plant and dose studies (see the **AP1000** plant DCD [2] Section1.5.1 and Appendix 3D.5.1.2) | | |
| 4.15 | 1 | National and international codes and standards that are used as design rules for items important to safety shall be identified and evaluated to determine their applicability, adequacy and sufficiency, and shall be supplemented or modified as necessary to ensure that the quality of the design is commensurate with the associated safety function. | | The design of **AP1000** plant SSCs meets this requirement as described in the **AP1000** plant DCD [2] Chapters 3 through 11. The **AP1000** plant DCD [2] Chapter 17 describes the design reliability assurance program.  Where applicable research and development program results obtained for the **AP600** configuration have been used to design the **AP1000** plant. This applies to materials, modular configuration of the plant and dose studies (see **AP1000** plant DCD [2] Section1.5.1 and Appendix 3D.5.1.2) | | |
| 4.16 | 1 | Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behavior of the plant is as expected. | | Testing has been performed to confirm the operation of new **AP1000** plant features as discussed in the **AP1000** plant DCD [2] Section 1.5. Pre-operational tests performed in the plant are discussed in Chapter 14. Periodic in-service tests are discussed in the **AP1000** plant DCD [2] Sections 3.9 and 16.1.  Where applicable research and development program results obtained for the **AP600** plant configuration have been used to design the **AP1000** plant. This applies to materials, modular configuration of the plant and dose studies (see **AP1000** plant DCD [2] Section 1.5.1 and Appendix 3D.5.1.2) | | |
| 4.16 (cont.) | 1 |  | | Westinghouse performed detailed assessment of applicability of **AP600** testing to the **AP1000** plant design which included:   * Development of phenomenon identification and ranking which assessed all DBAs to determine phenomenon that occurs during different stages of the DBAs and their importance to analyzing the DBAs. * Performing scaling assessments of **AP600** plant tests to determine their applicability to **AP1000** plant design.   In addition, additional testing at Oregon State University was performed to confirm that the **AP600** plant tests are applicable to the **AP1000** plant design.  The testing confirmed that the computer codes verified for **AP600** plant can be used for the **AP1000** plant design. Industry experts and the US NRC performed independent reviews and agreed with the conclusions. | | |
| 4.16 (cont.) | 1 |  | | The **AP600** plant test program included:  **Separate Effects Component / Subsystem Tests**   * Reactor coolant pump tests * Passive residual heat removal heat exchanger test * Core makeup tank test * Containment water distribution test * Containment shell heat and mass transfer tests * Containment cooling wind tunnel tests * Departure from nucleate boiling tests * Automatic depressurization system test (full scale)   **Integral Systems Tests**   * Integral passive containment cooling test * Large scale integral passive containment cooling test * Full height, full pressure integral systems test * Long term cooling integral systems test | | |
|  |  | **Requirement 10: Safety assessment**  **Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets requirements for manufacture and for construction, and as built, as operated and as modified.** | | The **AP1000** plant DCD [2] as a whole provides a comprehensive safety assessment. (see **AP1000** plant DCD [2] Appendix 1B, Chapters: 15, 17, 19) | | |
| 4.17 | 1 | The safety assessments10 shall be commenced at an early point in the design process, with iteration between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses.  *Footnote: 10 Requirements on safety assessment for facilities and activities are established in GSR Part 4 (Rev. 1) [2].* | | See the **AP1000** plant DCD [2] Section 19.1 which describes the iterative design process used with respect to the PRA. A similar process was carried out using deterministic safety analysis. | | |
| 4.18 | 1 | The safety assessments shall be documented in a form that facilitates independent evaluation. | | The **AP1000** plant DCD [2] as a whole provides a comprehensive **AP1000** plant safety assessment in a form that facilitates independent evaluation, and has been evaluated by the US NRC, the Chinese NNSA (preliminary and final safety analysis report), and by the UK safety authority as part of their GDA Step 4 process. For that process, the **AP1000** plant PCSR [19] was used as the basis of the assessment. This document presents the safety assessment of the **AP1000** plant in a format consistent with the UK regulatory requirements but is based on the same analyses as those presented in [2]. | | |
|  |  | **Requirement 11: Provision for construction**  **Items important to safety for a nuclear power plant shall be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required level of safety.** | | Westinghouse has conducted the **AP1000** plant design development under its recognized QMS and has taken prime responsibility for safety during the design development. This QMS and those of other participating organizations are applied in **AP1000** plant project implementations to ensure design specifications are met. Refer to the **AP1000** plant DCD [2] Section 17.3. | | |
| 4.19 | 1 | In the provision for construction and operation, due account shall be taken of relevant experience that has been gained in the construction of other similar plants and their associated structures, systems and components. Where best practices from other relevant industries are adopted, such practices shall be shown to be appropriate to the specific nuclear application. | | The **AP1000** plant design is based largely on experience from the existing Westinghouse PWR plants. Some structures in the **AP1000** plant are concrete-filled steel structures. This type of structure has not been commonly used in the nuclear industry. Use of this type of structure for the specific **AP1000** plant applications is shown to be appropriate in the **AP1000** plant DCD [2] Section 3.8 and Appendix 3H.  The constructability of the AP1000 plant structures using a quality-assured approach is established as part of the design. Westinghouse works closely with its construction partners. Construction, planning, and constructability reviews were performed concurrently with the civil engineering design. Lessons learned from earlier and ongoing construction projects are incorporated back into the design. Therefore, the construction process will be improved as a result of **AP1000** plant construction experience. | | |
|  |  | **Requirement 12: Features to facilitate radioactive waste management and decommissioning**  **Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive waste management and the future decommissioning and dismantling of the plant.** | | The **AP1000** plant DCD [2] Chapters 11 and 12 describe **AP1000** plant features that facilitate radioactive waste management.  In particular, the **AP1000** plant DCD [2] Section 12.1.2 and its subparagraphs described how the **AP1000** plantdesign accounts for ALARA .The increased reliability and durability of the components reduces not only the doses the workers might be exposed to, but also the maintenance of the components themselves, thus the volume of waste (contaminated/activated components) produced.  Plant decommissioning is not addressed in the **AP1000** plant DCD [2] but has been addressed for the UK in the **AP1000** plant ER and PCSR [6 & 20]. Waste minimization is an inherent part of waste management. The basic **AP1000** plant design principles minimize the creation of radwaste during operations and decommissioning. The **AP1000** plant was designed with fewer valves, pipes, and other components so less waste will be generated during maintenance activities (repair and replacement) and decommissioning. | | |
| 4.20 | 1 | In particular, the design shall take due account of:  (a) The choice of materials, so that amounts of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated;  (b) The access capabilities and the means of handling that might be necessary;  (c) The facilities necessary for the management (i.e. segregation, characterization, classification, pretreatment, treatment and conditioning) and storage of radioactive waste generated in operation and provision for managing the radioactive waste generated in the decommissioning of the plant. | | (a) The **AP1000** plant DCD [2] Chapter 11 describes the **AP1000** plant design features that facilitate radioactive waste management, while Section 12.3 describe the design features for ALARA. As described in the latter, equipment specifications for components exposed to high temperature reactor coolant contain limitations on the cobalt content of the base metal. The **AP1000** plant ER [6], Sections 3.5.1 and 3.5.4 further discuss how waste generation is minimized by design.  (b) The **AP1000** plant design takes into consideration means for accessing and handling contaminated components and materials. For example, access and handling of the CVS and spent fuel pool cooling system filters and discussed in the **AP1000** plant DCD [2] Section 11.4.2.3.2. To reduce the workers dose exposure (see **AP1000** plant DCD [2] Chapters 11, 12) remotely handled tools are used to handle the contaminated/activated components and materials.  (c) The **AP1000** plant DCD [2] Chapters 11 and 12 address radioactive waste management and radiation protection. The **AP1000** plant ER [6], Chapter 3 further discusses how radioactive management has been addressed in the **AP1000** plant design. The **AP1000** plant has been designed considering ALARA principles both during the plant operational life. Plant decommissioning is not addressed in the **AP1000** plant DCD [2] but has been addressed for the UK in the **AP1000** plant ER and PCSR [6 & 20]. | | |
| **5.0** |  | **GENERAL PLANT DESIGN** | |  | | |
|  |  | **DESIGN BASIS** | |  | | |
|  |  | **Requirement 13: Categories of plant states**  **Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis of their frequency of occurrence at the nuclear power plant.** | | Per the **AP1000** plant DCD [2] Chapter 15: The ANSI 18.2 classification is used for the **AP1000** plant which divides plant conditions into four categories according to anticipated frequency of occurrence and potential radiological consequences to the public. The four categories are as follows:   * Condition I: Normal operation and operational transients * Condition II: Faults of moderate frequency * Condition III: Infrequent faults * Condition IV: Limiting faults   The basic principle applied in relating design requirements to each of the conditions is that the most probable occurrences should yield the least radiological risk, and those extreme situations having the potential for the greatest risk should be those least likely to occur.  See also Section 5.0 of this document. | | |
| 5.1 | 1 | The plant states shall typically cover:  (a) Normal operation;  (b) Anticipated operational occurrences, which are expected to occur over the lifetime of the plant;  (c) Design basis accidents;  (d) Design extension conditions including accidents with core melting. | | See response for Requirement 13 regarding normal operation, AOOs and DBAs and Section 5.0 of this document.  Regarding DEC, PRA [4] and deterministic studies have been performed to define design measures to decrease the core damage frequency and large release frequency and prevent or mitigate events considered beyond design basis (e.g., ATWS, multiple steam generator tube rupture, and core melt sequences).  DECs including accidents with significant degradation of the reactor core are addressed in the **AP1000** plant DCD [2] Chapter 19 (PRA) and the PRA [4] (e.g., Chapter 34 (Severe Accident Phenomena Treatment), Chapter 39 (In-vessel Retention of Molten Core Debris)). | | |
| 5.2 | 1 | Criteria shall be assigned to each plant state, such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence. | | See response for Requirement 13. | | |
|  |  | **Requirement 14: Design basis for items important to safety**  **The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.** | | SSCs in the **AP1000** plant are classified according to nuclear safety classification, quality groups, seismic category, and codes and standards. The **AP1000** plant DCD [2] Section 3.2 provides the classification of SSCs. The design basis for items important to safety are specified in the **AP1000** plant DCD [2] for each system and their reliability and functionality have been considered in both the PRA (see **AP1000** plant DCD [2] Chapter 19) and deterministic safety analyses (see **AP1000** plant DCD [2] Chapters 15 and 6), as part of the design process.  Hazards (external and internal) are taken in account and are described in the **AP1000** plant DCD [2] Sections 3.3 through 3.7. | | |
| 5.3 | 1 | The design basis for each item important to safety shall be systematically justified and documented. The documentation shall provide the necessary information for the operating organization to operate the plant safely. | | The **AP1000** plant DCD [2] and the associated engineering documentation provide the necessary information for the operating organization to operate the plant safely. | | |
|  |  | **Requirement 15: Design limits**  **A set of design limits consistent with the key physical parameters for each item important to safety for the nuclear power plant shall be specified for all operational states and for accident conditions.** | | The **AP1000** plant design limits for SSCs important to safety are established for operational states and DBAs as discussed in the **AP1000** plant DCD [2] Chapters 3 through 12 and summarized in the plant Technical Specifications in Chapter 16. Technical Specifications are a dynamic set of plant parameters, associated limits and conditions for plant operation, and associated SSCs, that provide the delivery of safety functions for the **AP1000** plant. Short term availability controls are also defined for the active DiD systems (the **AP1000** plant DCD [2] Section 16.3). | | |
| 5.4 | 1 | The design limits shall be specified and shall be consistent with relevant national and international standards and codes, as well as with relevant regulatory requirements. | | Industrial Codes and Standards are obtained and used in the **AP1000** plant design as discussed in response to Requirement 9. Specific application of industrial codes and standards is provided in various sections of the **AP1000** plant DCD [2].  In addition to the internal verification, the **AP1000** plant design has been reviewed by various safety authorities, such as the US NRC, the UK ONR and the Chinese NNSA. | | |
|  |  | **Requirement 16: Postulated initiating events**  **The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.** | | The **AP1000** plant DCD [2] Chapter 15 describes the basis for the set of postulated initiating events considered as deterministic DBEs. The **AP1000** plant DCD [2] Chapter 19 (PRA) describes the process for identifying and assessing a comprehensive set of initiating events.  The **AP1000** plant safety assessment was also reviewed by the UK safety authority as part of their GDA Step 4 process. For that process, the **AP1000** plant PCSR [19] was used as the basis of the assessment. This document presents the safety assessment of the **AP1000** plant in a format consistent with the UK regulatory requirements, including for the identification of postulated initiating events, but is based on the same analyses as those presented in [2]. | | |
| 5.5 | 1 | The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analyses and probabilistic safety analyses shall be provided to show that all foreseeable events have been considered. | | The **AP1000** plant DCD [2] Section 15.0 provides the list of events considered in ANSI 18.2 Categories I through IV. The initiating event and event trees in the **AP1000** plant DCD [2] Chapter 19 **AP1000** plant PRA identify a comprehensive set of initiating events and are based on evaluations that included a review of PWR operating experience, past PRAs, and consideration of **AP1000** plant specific features. | | |
| 5.6 | 1 | The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states. | | See response for Requirement 5.5. Human factors that may affect plant operations are discussed in the **AP1000** plant DCD [2] Chapter 18. The impacts resulting from human error are described in the **AP1000** plant DCD [2] Chapter 15 and the PRA [4]. Also, the **AP1000** plant has been evaluated for events that can occur during shutdown conditions as shown in the **AP1000** plant DCD [2] Chapter 19. The Technical Specifications (see **AP1000** plant DCD [2] Section 16.1) specifically address the available equipment requirements during startup, shutdown, and maintenance. | | |
| 5.7 | 1 | An analysis of the postulated initiating events for the plant shall be made to establish the preventive measures and protective measures that are necessary to ensure that the required safety functions will be performed. | | The **AP1000** plant DCD [2] Chapters 6, 15, and 19 provide the **AP1000** plant analyses of the postulated initiating events. | | |
| 5.8 | 1-5 | The expected behaviour of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority:  (1) A postulated initiating event would produce no safety significant effects or would produce only a change towards safe plant conditions by means of inherent characteristics of the plant.  (2) Following a postulated initiating event, the plant would be rendered safe by means of passive safety features or by the action of systems that are operating continuously in the state necessary to control the postulated initiating event.  (3) Following a postulated initiating event, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the postulated initiating event  (4) Following a postulated initiating event, the plant would be rendered safe by following specified procedures. | | This priority of behaviors is exhibited by the **AP1000** plant analyses included in the **AP1000** plant DCD [2] Chapters 15 and 19. For example:   1. Negative moderator temperature coefficient acts to limit reactor power for events with moderator temperature increase. 2. The normal operating active systems are capable of maintaining safe conditions for many initiating events. In case of an initiating event taking place, the DiD systems actuates in order to prevent the safety passive system to actuates (see response for Paragraph 2.13). 3. The **AP1000** plant passive safety systems render the plant safe for the DBEs. 4. The emergency operating procedures provide guidance for successful operator response to event sequences. | | |
| 5.9 | 1 | The postulated initiating events used in the development of the performance requirements for the items important to safety in the overall safety assessment and detailed analysis of the plant shall be grouped into a specified number of representative event sequences that identify bounding cases and that provide the basis for the design and the operational limits for items important to safety. | | This grouping of **AP1000** plant DBEs is discussed in the **AP1000** plant DCD [2] Chapter 15. | | |
| 5.10 | 1 | A technically supported justification shall be provided for exclusion from the design of any initiating event that is identified in accordance with the comprehensive set of postulated initiating events. | | A comprehensive set of initiating events are considered in the **AP1000** plant PRA [4] and the risk associated has been evaluated in the **AP1000** plant DCD [2] Chapters 15 and 19. This set of initiating events is based on review of PWR operating experience, past PRAs, and consideration of **AP1000** plant specific features. | | |
| 5.11 | 1 | Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions. | | Engineered safety features are actuated automatically in response to initiating events. These engineered safety features protect the public in the event of an accidental release of radioactive fission products from the RCS. The engineered safety features function to localize, control, mitigate, and terminate such accidents and to maintain radiation exposure levels to the public below applicable limits and guidelines, such as Title 10 of the Code of Federal Regulations Part 50.34 (10 CFR 50.34).  The **AP1000** plant Engineered Safety Features are as defined in the **AP1000** plant DCD [2] Chapter 6. | | |
| 5.12 | 1 | Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems or other operator actions. For such cases, the time interval between the detection of the abnormal event or accident and the required action shall be sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process. | | Generally the need for operator actions has been greatly reduced in the **AP1000** plant and such actions are typically not required to place the plant in a long‑term safety shutdown condition. The human system interface design (see **AP1000** plant DCD [2] Chapter 18) includes the appropriate plant displays, alarms, and controls needed to support a broad range of expected power generation, shutdown, and accident mitigation operations. In addition, the procedures for normal operation, alarm response, and abnormal and emergency responses; as well as the severe accident management guidelines have been developed to prevent erroneous operation or incorrect diagnosis. Also see response for Requirement 5.15. | | |
| 5.13 | 1 | The operator actions that are necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment. | | See response for Paragraph 5.12. | | |
| 5.14 | 1 | The design shall specify the necessary provision of equipment and the procedures necessary to provide the means for keeping control over the plant and for mitigating any harmful consequences of a loss of control. | | See response for Paragraph 5.12. | | |
| 5.15 | 1 | Any equipment that is necessary for actions to be taken in manual response and recovery processes shall be placed at the most suitable locations to ensure its availability at the time of need and to allow safe access to it under the environmental conditions anticipated. | | This is incorporated in the **AP1000** plant design as discussed in the **AP1000** plant DCD [2] Chapter 18 Human Factors. The **AP1000** plant design includes a few components intended to be manually implemented to continue safety functions post 72 hours following a DBE. These components are located for safe access by the operating staff. | | |
|  |  | **Requirement 17: Internal and external hazards**  **All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.** | | Internal and external hazards have been considered in the **AP1000** plant design as described in various parts of the **AP1000** plant DCD [2] Chapters 2 through 12. Human factors have been evaluated and are discussed in the **AP1000** plant DCD [2] Chapter 18, and in the **AP1000** plant DCD [2] Chapter 15 (e.g., Sections 15.0.13 and 19.30).  Internal and external hazards were also reviewed for the **AP1000** plant GDA in the UK, as documented in Chapters 11 and 12 of the **AP1000** plant PCSR [19]. | | |
| 5.15A | 1 | Items important to safety shall be designed and located, with due consideration of other implications for safety, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards. | | The **AP1000** plant design includes redundancy and physical separation of components as necessary to fulfill the plant’s safety functions. See response for Requirement 5.17, and compliance to US NRC GDCs 5, 13, 22, 24, 26 [12]. Design for external hazard is also discussed in the **AP1000** plant DCD [2] Chapter 3 and in [16]. | | |
| 5.15B | 1 | For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously. | | This is assessed on a site specific basis. However, it is noted that each **AP1000** plant unit at a site is a stand-alone design. | | |
|  |  | **Internal hazards** | |  | | |
| 5.16 | 1 | The design shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact, and release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised. | | The **AP1000** plant design provides protection for internal hazards. The **AP1000** plant DCD [2] Sections 3.3 (Wind and Tornado), 3.4 (External Flood), 3.5 (Missiles), 3.6 (Rupture of Piping), 19.56 (Internal Flood), 19.57 (Internal Fire), 19.58 (External Wind, Floods), describes design considerations for wind, flood, fire, missiles, and pipe rupture hazards. Leak before break criteria for **AP1000** plant piping is addressed in the **AP1000** plant DCD [2] Appendix 3B. Aircraft impact is addressed in the **AP1000** plant DCD [2] Appendix 19F. | | |
|  |  | **External hazards** | |  | | |
| 5.17 | 1 | The design shall include due consideration of those natural and human induced external events11 (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.  *Footnote: 11 Requirements on site evaluation for nuclear installations are established in IAEA Safety Standards Series No. NS-R-3 (Rev. 1), Site Evaluation for Nuclear Installations [10].* | | The design of **AP1000** plant nuclear safety systems and engineered safety features includes allowances for natural environmental disturbances such as earthquakes, floods, and storms at the station site. The nuclear island structures are designed to withstand the effects of natural phenomena such as hurricanes, floods, tornados, tsunamis, and earthquakes without loss of capability to perform safety functions. Design for natural phenomena is based on the industry standards as described in the **AP1000** plant DCD [2] Chapters 2 and 3. Those SSCs vital to the shutdown capability of the reactor are designed to withstand the envelope of probable natural phenomena described in the **AP1000** plant DCD [2] Chapter 2. These SSCs are sufficient to bring and maintain the reactor in safe shutdown, and to cool the spent fuel pool, for at least 72 hours following an event.  Specific sites are evaluated with respect to the **AP1000** plant site envelope to assure site specific safety capabilities. | | |
| 5.17 (cont.) | 1 |  | | The design of **AP1000** plant takes into account the potential effects of the impact of a large commercial aircraft, as discussed in the **AP1000** plant DCD [2] Appendix 19F. The impacting aircraft analyzed is based upon the impulse time curve provided by the US NRC in July 2007, which also include analyses of large commercial aircrafts. The assessment concludes that **AP1000** plant can continue to provide adequate protection of the public health and safety with respect to aircraft impact as defined by the US NRC. The aircraft impact would not inhibit the **AP1000** plant’s core cooling capability, containment integrity, spent fuel pool integrity, or adequate spent fuel cooling based on best estimate calculations.  In addition consideration of post Fukushima events, not included in the **AP1000** plant DCD [2], have been separately addressed for the **AP1000** plant design [14][15][16], and in Appendix 12B of the **AP1000** plant PCSR [19]. | | |
| 5.18 | 1 | This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A. | | See response for Paragraph 5.15A. | | |
| 5.19 | 1 | Features shall be provided to minimize any interactions between buildings containing items important to safety (including power cabling and control cabling) and any other plant structure as a result of external events considered in the design. | | See response for Requirements 5.17 and 5.18.  Also, see **AP1000** plant DCD [2] Section 3.7 (Seismic Design). Seismic Category I SSCs are designed to withstand the effects of the safe shutdown earthquake event and to maintain the specified design functions. Seismic Category II and nonseismic structures are designed or physically arranged (or both) so that the safe shutdown earthquake could not cause unacceptable structural interaction with or failure of seismic Category I SSCs. | | |
| 5.20 | 1 | This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A. | | See response for Paragraph 5.15A. | | |
| 5.21 | 1 | The seismic design of the plant shall provide for an adequate margin to protect items important to safety against levels of hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects12.  *Footnote: 12 A ‘cliff edge effect’, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.* | | The **AP1000** plant is designed for a safe shutdown earthquake defined by a peak ground acceleration of 0.3g and the design response spectra specified in the **AP1000** plant DCD [2] Section 3.7.1.1. This is intended to envelope most sites and provide safety margin. An **AP1000** plant seismic margin analysis is also provided in the **AP1000** plant DCD [2] Section 19.55 and shows that there are no “cliff-edge effects” by demonstrating that the critical SSCs have a high confidence of a low probability of failure for seismic events equal to or greater than 0.5g. | | |
| 5.22 | 1 | This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15B. | | See response for Paragraph 5.15B. | | |
|  |  | **Requirement 18: Engineering design rules**  **The engineering design rules for items important to safety at a nuclear power plant shall be specified and shall comply with the relevant national or international codes and standards and with proven engineering practices, with due account taken of their relevance to nuclear power technology.** | | The Westinghouse **AP1000** plant design is based on the safety criteria, regulatory guidelines, and industry codes and standards employed in US nuclear power PWR facilities. The conformance of the **AP1000** plant SSCs with the US NRC GDC is discussed in the **AP1000** plant DCD [2] Section 3.1.  Industrial Codes and Standards are obtained and used in the **AP1000** plant design as discussed in response to Requirement 9. Specific application of industrial codes and standards is provided in various sections of the **AP1000** plant DCD [2].  In addition to the internal verification, the **AP1000** plant design has been reviewed by various safety authorities, such as the US NRC, the UK ONR and the Chinese NNSA. | | |
| 5.23 | 1 | Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of a nuclear power plant to ensure that the fundamental safety functions are achieved for all operational states and for all accident conditions. | | Westinghouse has conducted the **AP1000** plant design development under its recognized QMS and has taken prime responsibility for safety during the design development. This QMS and those of other participating organizations are applied in **AP1000** plant project implementations to ensure design specifications are met. Engineered safety features can be found in the **AP1000** plant DCD [2] Chapter 6. In addition, refer to the **AP1000** plant DCD [2] Section 17.3. | | |
|  |  | **Requirement 19: Design basis accidents**  **A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.** | | The DBAs for the **AP1000** plant are as defined in the **AP1000** plant DCD [2] Chapters 6 and 15. | | |
| 5.24 | 1 | Design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design basis accident conditions, with the objective of returning the plant to a safe state and mitigating the consequences of accidents. | | Mitigating DBAs is the role of **AP1000** plant engineered safety features as discussed in the **AP1000** plant DCD [2] Chapter 6. | | |
| 5.25 | 1 | The design shall be such that for design basis accident conditions, key plant parameters do not exceed the specified design limits. A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological impacts, on or off the site, and do not necessitate any off-site intervention measures. | | **AP1000** plant response to DBAs is described in the **AP1000** plant DCD [2] Chapters 6 and 15, including compliance with radiological limits (off site measurement is addressed in the response for Paragraph 5.31). Plant operational limits (Technical Specifications) are provided in the **AP1000** plant DCD [2] Chapter 16. | | |
| 5.26 | 1 | The design basis accidents shall be analysed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis. | | **AP1000** plant DBAs are analyzed in a conservative manner as discussed in the **AP1000** plant DCD [2] Chapters 6 and 15. **AP1000** plant PRAs have been performed and are discussed in the **AP1000** plant DCD [2] Chapter 19. | | |
|  |  | **Requirement 20: Design extension conditions**  **A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant’s capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.** | | This process has been applied in the design of **AP1000** plant features as part of the PRA described in the **AP1000** plant DCD [2] Chapter 19.  PRA and deterministic studies have been performed to define design measures to decrease the core damage frequency and large release frequency and prevent or mitigate events considered beyond design basis (e.g., ATWS, multiple steam generator tube rupture, and core melt sequences).  Beyond DBAs, or DECs in European terminology, including accidents with significant degradation of the reactor core are addressed in the **AP1000** plant DCD [2] Chapter 19 (PRA) and the PRA [4] (e.g. Chapter 34 (Severe Accident Phenomena Treatment), Chapter 39 (In-vessel Retention of Molten Core Debris)). Aircraft impact is addressed in the **AP1000** plant DCD [2] Appendix 19F. In addition, consideration of post-Fukushima events, not included in the **AP1000** plant DCD [2], have been separately addressed for the **AP1000** plant design [14][15][16], and in Appendix 12B of the **AP1000** plant PCSR [19]. | | |
| 5.27 | 1 | An analysis of design extension conditions for the plant shall be performed13. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered as design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequences of, a severe accident, or to maintain the integrity of the containment. These additional safety features for design extension condition, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’14. The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach. | | The **AP1000** plant DCD [2] Chapter 19 provides the PRA showing the extremely low likelihood of serious radiological consequences and that mitigation measures are effective for severe accidents.  DECs including accidents with significant degradation of the reactor core as a result of multiple failures are addressed in the **AP1000** plant DCD [2] Chapter 19 (PRA) and the PRA [4] (e.g. Chapter 34 (Severe Accident Phenomena Treatment), Chapter 39 (In‑vessel Retention of Molten Core Debris)).  Reactor vessel integrity is addressed in the **AP1000** plant DCD [2] Section 5.3.4. The PRA [4] show the low probability of failure for the **AP1000** plant steel containment vessel. The **AP1000** plant design has been developed based on extensive use of deterministic and probabilistic analyses to determine that radiation risks arising throughout the plant lifecycle are ALARA. As a result the core melt frequency and large release frequency for the **AP1000** plant are at least two orders of magnitude lower than required by the safety authorities. | | |
| 5.27 (cont.) | 1 | *Footnotes: 13 The analysis of design extension conditions for the plant could be performed by means of a best estimate approach (more stringent approaches may be used according to States’ requirements).*  *14 The possibility of certain conditions arising may be considered to have been ‘practically eliminated’ if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.* | | Dose calculations have been performed in accordance with US (see **AP1000** plant DCD [2] Chapter 15 and 19) and European (e.g., EUR) requirements for both DBA [9] and DEC [10] events to ensure that radioactive releases are within limits.  EPS-GW-GL-701, **AP1000** Evaluation of Western European Nuclear Regulators’ Association (WENRA) Safety Objectives for New Power Reactors [17] describes the compliance of the **AP1000** plant design to WENRA Safety Objectives O2. (Accidents without Core Melt) and 03 (Accidents with Core Melt). **AP1000** plant design accidents with early and large releases have been practically eliminated. Design provisions ensure containment integrity with high probability in the unlikely event of core melt. However, in the unlikely event of core melt **AP1000** plant in-vessel retention ensures the core successfully remains in the reactor vessel (see **AP1000** plant DCD [2] Section 19.39 and PRA Chapter 39).  Also see the responses to Requirement 20, and Paragraph 5.30. | | |
| 5.28 | 1 | The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences. | | The **AP1000** plant design has been developed based on extensive use of deterministic and probabilistic analyses to determine that radiation risks arising throughout the plant lifecycle are ALARA. (see **AP1000** plant DCD [2] Chapters 6, 15, and 19).  Also see the response for Paragraphs 5.29 and 5.30. | | |
| 5.29 | 1 | The analysis undertaken shall include identification of the features that are designed for use in, or that are capable15 of preventing or mitigating, events considered in the design extension conditions. These features:   1. Shall be independent, to the extent practicable, of those used in more frequent accidents; 2. Shall be capable of performing in the environmental conditions pertaining to these design extension conditions, including design extension conditions in severe accidents, where appropriate; 3. Shall have reliability commensurate with the function that they are required to fulfill.   *Footnote: 15 For returning the plant to a safe state or for mitigating the consequences of an accident, consideration could be given to the full design capabilities of the plant and to the temporary use of additional systems.* | | For non-core melt DEC, the diversity incorporated into the **AP1000** plant passive safety systems (based on the PRA insights) allow them to provide diverse passive means of mitigation of the most frequent occurrences. This design approach provides, for the most frequent events, the three diverse lines of protection listed below:   * Primary means: passive safety systems (credited to mitigate postulated initiating events in the design basis analyses) * Secondary means: diverse passive safety systems (credited in the PRA) * Tertiary means: active DiD systems (credited in the PRA)   This approach provides the basis for the consideration of multiple failure events (such as DEC) in the **AP1000** plant design. The environmental conditions for those DEC are similar to the DBA conditions for which the passive systems are qualified.  For core melt DEC, the AP1000 plant DCD [2] Appendix 19D (equipment survivability assessment) evaluates the availability of equipment and instrumentation used during a severe accident to achieve a controlled, stable state after core damage under the unique containment environments. | | |
| 5.29  (cont.) | 1 |  | | The **AP1000** plant D-RAP includes a design evaluation of the **AP1000** plant and identifies the aspects of plant operation, maintenance, and performance monitoring pertinent to risk-significant SSCs. In addition to the PRA, deterministic tools, industry sources, and expert opinion are used to identify and prioritize risk‑significant SSCs. Refer to the **AP1000** plant DCD [2] Section 17.4. Also see the response for Paragraph 5.31. | | |
| 5.30 | 1 | In particular, the containment and its safety features shall be able to withstand extreme scenarios that include, among other things, melting of the reactor core. These scenarios shall be selected using engineering judgement and input from probabilistic safety assessments. | | One of the key **AP1000** plant severe accident design features is the capability to retain the core debris within the reactor vessel for a large number of severe accident sequences by ensuring that the reactor cavity is flooded, submerging the outer surface of the reactor vessel. The heat removal capability of the water on the external surface of the reactor vessel prevents the reactor vessel wall from reaching temperatures where failure of the reactor vessel could occur. This primary benefit of in-vessel retention of the core is that ex‑vessel severe accident phenomena associated with relocation of core debris to the containment, which can be a dominant containment failure mechanism, are physically prevented.  Despite the practical elimination of these events, analysis has been performed to demonstrate additional levels of defense to large early releases. For example, Section 19B.5 of the **AP1000** plant DCD [2] presents deterministic analyses performed to consider the unlikely case of a core melt not retained in the vessel. The discussion concludes that such a core melt would not likely result in containment failure due to effects of direct containment heating from a high pressure melt ejection, steam explosion, or core concrete interactions.  Hydrogen challenges are also addressed in the **AP1000** plant. The control hydrogen system, and the equipment survivability for severe accident mitigation are discussed in the AP1000 plant DCD [2] Sections 19.16 and Appendix 19B, respectively. | | |
| 5.31 | 1 | The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’16.  *Footnote: 16 The possibility of certain conditions arising may be considered to have been ‘practically eliminated’ if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.* | | The **AP1000** plant PRA described in the **AP1000** plant DCD [2] Chapter 19 shows that severe accidents with large or early releases can be considered to have been practically eliminated by virtue of their extremely low frequency. The **AP1000** plant DCD [2] Chapter 1 Appendix 1B provides assessment of additional design measures not included in the **AP1000** plant design, showing these additional measures would not significantly reduce radiological consequences. Offsite intervention measures are decided on a site specific basis. The **AP1000** plant design provides significant time before offsite intervention is needed (at least 72 hr). Furthermore, the design includes margin to the US utility goal for site boundary whole‑body dose and the acute red bone marrow dose (<25 rems (0.25 sieverts), at a frequency not to exceed 1x10-6 per year).  EPS-GW-GL-701, **AP1000** Evaluation of Western European Nuclear Regulators’ Association (WENRA) Safety Objectives for New Power Reactors [17] describes the compliance of the **AP1000** plant design to WENRA Safety Objective 03 (Accidents with Core Melt). | | |
| 5.31A | 1 | The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures. | | See response for Paragraph 5.31 and EPS-GW-GL-701, **AP1000** Evaluation of Western European Nuclear Regulators’ Association (WENRA) Safety Objectives for New Power Reactors [17] regarding compliance of the **AP1000** plant design to WENRA Safety Objective 03 (Accidents with Core Melt). | | |
|  |  | **Combinations of events and failures** | |  | | |
| 5.32 | 1 | Where the results of engineering judgement, deterministic safety assessments and probabilistic safety assessments indicate that combinations of events could lead to anticipated operational occurrences or to accident conditions, such combinations of events shall be considered to be design basis accidents or shall be included as part of design extension conditions, depending mainly on their likelihood of occurrence. Certain events might be consequences of other events, such as a flood following an earthquake. Such consequential effects shall be considered to be part of the original postulated initiating event. | | The **AP1000** plant PRA, as summarized in the **AP1000** plant DCD [2] Chapter 19, provides a systematic evaluation of events and failures. This evaluation ensures that combinations of events that are reasonably probable are considered. Consequential failures including loss of offsite power when a reactor trip occurs are considered in deterministic DBEs.  In addition some severe phenomena including aircraft crash and consideration of post Fukushima events, not included in the **AP1000** plant DCD [2], have been separately addressed for the **AP1000** plant design [14][15][16] and in Appendix 12B of the **AP1000** plant PCSR [19]. | | |
|  |  | **Requirement 21: Physical separation and independence of safety systems**  **Interference between safety systems or between redundant elements of a system shall be prevented by means such as physical separation, electrical isolation, functional independence and independence of communication (data transfer), as appropriate**. | | Such design measures are applied in the **AP1000** plant design, for example see **AP1000** plant DCD [2] Chapter 7. Also see the response for Paragraph 2.13 where diversity between the DiD and the safety systems is discussed. | | |
| 5.33 | 1 | Safety system equipment (including cables and raceways) shall be readily identifiable in the plant for each redundant element of a safety system. | | The **AP1000** plant design provides for equipment identification. | | |
|  |  | **Requirement 22: Safety classification**  **All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.** | | SSCs in the **AP1000** plant are classified according to nuclear safety classification, quality groups, seismic category, and codes and standards. The **AP1000** plant DCD [2] Section 3.2 provides the classification of SSCs.  Also refer to Section 5.0 of this document. | | |
| 5.34 | 1 | The method for classifying the safety significance of items important to safety shall be based primarily on deterministic methods complemented where appropriate, by probabilistic methods, with due account taken of factors such as:  (a) The safety function(s) to be performed by the item;  (b) The consequences of failure to perform a safety function;  (c) The frequency with which the item will be called upon to perform a safety function;  (d) The time following a postulated initiating event at which, or the period for which, the item will be called upon to perform a safety function. | | The **AP1000** plant assignment of safety classification and use of codes and standards conforms to the requirements of 10 CFR 50.55a for the development of a Quality Group classification and the use of codes and standards. The classification system provides a means of identifying the extent to which SSCs are related to safety-related and seismic requirements. The classification system provides an easily recognizable means of identifying the extent to which SSCs are related to American Nuclear Society nuclear safety classification, US NRC quality groups, ASME Code, Section III classification, seismic category and other applicable industry standards, as shown in the **AP1000** plant DCD [2] Table 3.2-3. See also Section 5.0 of this document. | | |
| 5.35 | 1 | The design shall be such as to ensure that any interference between items important to safety will be prevented, and in particular that any failure of items important to safety in a system in a lower safety class will not propagate to a system in a higher safety class. | | **AP1000** plant components are classified down to the replacement part level according to the definitions and criteria of the classification system (see **AP1000** plant DCD [2] Section 3.2). A single item or portion thereof, which provides two or more functions of different classes, is classified according to the most stringent function. Different portions of the same SSC may perform different functions and be assigned to different equipment classes if the SSC contains a suitable interface boundary (see **AP1000** plant DCD [2] Chapter 7).  [18] also demonstrates the absence of adverse interactions between the **AP1000** plant safety systems and systems of lower safety classes. | | |
| 5.36 | 1 | Equipment that performs multiple functions shall be classified in a safety class that is consistent with the most important function performed by the equipment. | | A single **AP1000** plant item or portion thereof, which provides two or more functions of different classes, is classified according to the most important function. | | |
|  |  | **Requirement 23: Reliability of items important to safety**  **The reliability of items important to safety shall be commensurate with their safety significance.** | | The **AP1000** Plant D-RAP includes a design evaluation of the **AP1000** plant and identifies the aspects of plant operation, maintenance, and performance monitoring pertinent to risk-significant SSCs. In addition to the PRA, deterministic tools, industry sources, and expert opinion are used to identify and prioritize those risk‑significant SSCs. Refer to the **AP1000** plant DCD [2] Section 17.4. | | |
| 5.37 | 1 | The design of items important to safety shall be such as to ensure that the equipment can be qualified, procured, installed, commissioned, operated and maintained to be capable of withstanding, with sufficient reliability and effectiveness, all conditions specified in the design basis of the items. | | **AP1000** plant equipment specifications follow the design requirements as discussed in the **AP1000** plant DCD [2] Chapters 3 through 12. Also see response for Paragraphs 3.0 through 3.6. | | |
| 5.38 | 1 | In the selection of equipment, consideration shall be given to both spurious operation and unsafe failure modes. Preference shall be given in the selection process to equipment that exhibits a predictable and revealed mode of failure and for which the design facilitates repair or replacement. | | **AP1000** plant equipment selection has considered potential for spurious operation and for unsafe failure modes. | | |
|  |  | **Requirement 24: Common cause failures**  **The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.** | | Common cause analysis is included in the **AP1000** plant PRA as stated in the **AP1000** plant DCD [2] Section 19.29. The PRA was used to define where and to what degree diversity needed to be incorporated into the **AP1000** plant SSCs.  The primary purpose of equipment qualification, as presented in the **AP1000** plant DCD [2] Appendix 3D is to reduce the potential for common mode failures due to anticipated environmental and seismic conditions. | | |
|  |  | **Requirement 25: Single failure criterion**  **The single failure criterion shall be applied to each safety group incorporated in the plant design.** | | The **AP1000** plant safety systems are designed to mitigate DBAs with a single failure, as defined in the **AP1000** plant DCD [2] Chapter 15. | | |
| 5.39 | 1 | Spurious action shall be considered to be one mode of failure when applying the single failure criterion17 to a safety group or safety system.  *Footenote: 17 A single failure is a failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it. The single failure criterion is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.* | | The **AP1000** plant is designed for spurious actions as single failures except in a few cases where specific features (such as power lockout, confirmatory open signals, or continuous position alarms) are applied to prevent such failures. | | |
| 5.40 | 1 | The design shall take due account of the failure of a passive component, unless it has been justified in the single failure analysis with a high level of confidence that a failure of that component is very unlikely and that its function would remain unaffected by the postulated initiating event. | | Failure of passive components has been considered in the **AP1000** plant design. Passive failure is discussed in the following **AP1000** plant DCD [2] sections: Section 1.9.5.3.2; Chapter 5; Sections 6.3; 6.3.5.2; 6.4.4; 9.1.3.12 and 16.1 (Technical Specification 16.B.3.7).  Furthermore, **AP1000** plant analyses consider passive failures as described in the **AP1000** plant DCD [2] Section 15.0.12.2. | | |
|  |  | **Requirement 26: Fail-safe design**  **The concept of fail-safe design shall be incorporated, as appropriate, into the design of systems and components important to safety.** | | The **AP1000** plant passive safety systems use only natural forces such as gravity, natural circulation, and compressed gas to make the systems work. A few valves are automatically realigned to initiate the passive safety system functions. To provide high reliability, many of these valves, as well as many of the containment isolation valves, are designed to be fail safe (actuate to their safety positions upon loss of power). See [14] for further details. | | |
| 5.41 | 1 | Systems and components important to safety shall be designed for fail-safe behaviour, as appropriate, so that their failure or the failure of a support feature does not prevent the performance of the intended safety function. | | See response for Requirement 26. | | |
|  |  | **Requirement 27: Support service systems**  **Support service systems that ensure the operability of equipment forming part of a system important to safety shall be classified accordingly.** | | The **AP1000** plant passive safety systems are significantly simpler than typical PWR safety systems since they contain significantly fewer components, reducing the required tests, inspections, and maintenance. They require no active support systems, such as ac power, cooling water system, heating ventilating and air conditioning, or instrument air system. In many cases they are fail safe and as a result, do not require any support systems including I&C or direct current power. A few of the passive system components do require I&C and direct current power for their initial alignment; where needed, batteries provide this direct current power and are classified as safety equipment (see Section 5.0 for more details).  For the active DiD systems, all systems required for their operation in mitigation of AOOs is also classified as DiD. These include the onsite standby diesel generators, the PLS, and various cooling systems, such as the service water system and the component cooling system. | | |
| 5.42 | 1 | The reliability, redundancy, diversity and independence of support service systems and the provision of features for their isolation and for testing their functional capability shall be commensurate with the significance to safety of the system that is supported. | | This is met by the **AP1000** plant design. For example, the I&C system (PMS, see **AP1000** plant DCD [2] Section 7.1.2) and direct current power system (IDS, see **AP1000** plant DCD [2] Section 8.3.2.1.1) that support the passive safety systems are designed as safety systems which are redundant and independent. | | |
| 5.43 | 1 | It shall not be permissible for a failure of a support service system to be capable of simultaneously affecting redundant parts of a safety system or a system fulfilling diverse safety functions, and compromising the ability of these systems to fulfil their safety functions. | | Multiple failures within the I&C (see **AP1000** plant DCD [2] Section 7.1.2) and direct current power system (see **AP1000** plant DCD [2] Section 8.3.2.1.1), that support the passive safety systems, are considered in the **AP1000** plant PRA (**AP1000** plant DCD [2] Chapter 19). A single failure of a component in a redundant system is not capable of affecting the other redundant components. | | |
|  |  | **Requirement 28: Operational limits and conditions for safe operation**  **The design shall establish a set of operational limits and conditions for safe operation of the nuclear power plant.** | | The **AP1000** plant DCD [2] Chapter 16 (Technical Specifications) provides the **AP1000** plant operational limits and conditions for safe operation. | | |
| 5.44 | 1-8 | The requirements and operational limits and conditions established in the design for the nuclear power plant shall include (Requirement 6 of IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [4]):  (a) Safety limits;  (b) Limiting settings for safety systems;  (c) Limits and conditions for normal operation;  (d) Control system constraints and procedural constraints on process variables and other important parameters;  (e) Requirements for surveillance, maintenance, testing and inspection of the plant to ensure that structures, systems and components function as intended in the design, to comply with the requirement for optimization by keeping radiation risks as low as reasonably achievable;  (f) Specified operational configurations, including operational restrictions in the event of the unavailability of safety systems or safety related systems;  (g) Action statements, including completion times for actions in response to deviations from the operational limits and conditions. | | The **AP1000** plant DCD [2] Chapter 16 (Technical Specifications) provides the defined Modes of Operation for the **AP1000** plant, the Safety Limits, the Limiting Conditions for Operation, and the Surveillance Requirements. This set of technical specifications is intended to be used as a guide in the development of the plant-specific technical specifications by the Plant Owner.  Also see response to Requirement 29 and Paragraph 4.11. | | |
|  |  | **DESIGN FOR SAFE OPERATION OVER THE LIFETIME OF THE PLANT** | |  | | |
|  |  | **Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety**  **Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.** | | The **AP1000** plant SSCs important to safety meet these requirements. Westinghouse has developed an initial test program, described in Chapter 14 of the AP1000 plant DCD [2] that is performed during initial startup of the AP1000 plant. The overall objective of the test program is to demonstrate that the plant has been constructed as designed, that the systems perform consistent with the plant design, and that activities culminating in operation at full licensed power including initial fuel load, initial criticality, and power ascension are performed in a controlled and safe manner.There are guiding criteria that have been used in the design of the plant for maintainability and for performing maintenance, testing, and surveillance activities. These criteria are based on input from utilities and industry groups, Westinghouse service experience, and input from the **AP1000** plant Executive US Builders Group (an informal entity of **AP1000** plant US utility customers). Inservice Inspection of Class 1 Components is discussed in the **AP1000** plant DCD [2] Section 5.2.4 and Inservice Inspection of Class 2, 3, and MC Components is discussed in the **AP1000** plant DCD [2] Section 6.6. Inservice testing of safety components is discussed in Section 3.9.6. | | |
|  |  | **Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety**  **(cont.)** | | Surveillance testing requirements are specified in the plant Technical Specifications as described in the **AP1000** plant DCD [2] Section 16.1. Maintainability of the AP1000 plant was assessed as part of the human factor assessment presented in the **AP1000** plant DCD [2] Chapter 18. The **AP1000** plant layout has taken into consideration required access for testing, maintainability, repair, replacement and in-service inspection of components. | | |
| 5.45 | 1 | The plant layout shall be such that activities for calibration, testing, maintenance repair or replacement, inspection and monitoring are facilitated and can be performed to relevant national and international codes and standards. Such activities shall be commensurate with the importance of the safety functions to be performed, and shall be performed without undue exposure of workers. | | See response for Requirements 29 and 78.  ALARA has been built into the design of civil structures, the fuel storage and handling and the auxiliaries systems (see **AP1000** plant DCD [2] Sections 6.1.2.1, 9.1.3.1, 9.3).  The **AP1000** plant layout has taken into consideration required access for testing, maintainability, repair, replacement and in-service inspection of components. This includes consideration of ALARA. Also see response to Requirement 5 which addresses ALARA in the **AP1000** plant design. | | |
| 5.46 | 1 | Where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed for performing such tasks with no significant reduction in the reliability of performance of the safety functions. Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions. | | Testing and maintenance requirements for components important to safety are outlined in the **AP1000** plant DCD [2], PRA [4], the Technical Specifications (**AP1000** plant DCD [2] Section 16.1) and the short term availability controls (**AP1000** plant DCD [2] Section 16.3). For example, testing and maintenance requirements for the following components are discussed in the following **AP1000** plant PRA [4] sections: passive residual heat removal heat exchanger (PRA Section 8.2.3), core makeup tank (PRA Section 9.1.3), accumulator (PRA Section 10.1.3), automatic depressurization (PRA Section 11.2.3), in‑containment refueling water storage tank (PRA Section 12.2.3), etc. These sections defined when it is appropriate to test and/or maintain the component during power operation and when it is required to perform the activities during plant shutdown. The **AP1000** plant component testing and maintenance philosophy ensures that tasks can be performed with no significant reduction in the reliability or performance of the component’s safety function(s).  Also see response for Requirement 29. | | |
| 5.47 | 1-3 | If an item important to safety cannot be designed to be capable of being tested, inspected or monitored to the extent desirable, a robust technical justification shall be provided that incorporates the following approach:  (a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified;  (b) Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures. | | This requirement is not applicable to the **AP1000** plant design. All important to safety components are capable of being tested, inspected and monitored to the extent desirable. See response for Paragraph 5.46 and Requirement 29 for additional information regarding testing, inspection and monitoring of **AP1000** plant “important to safety” components. | | |
|  |  | **Requirement 30: Qualification of items important to safety**  **A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.** | | The **AP1000** plant meets these requirements as discussed in the **AP1000** plant DCD [2] Section 3.11, “Environmental Qualification of Mechanical and Electrical Equipment.” Appendix 3D provides the methodology for qualification of **AP1000** plant safety equipment. The equipment environmental qualification program ensures that components are designed and qualified taking into consideration the most extreme operational conditions (whether it be during accident conditions or maintenance and testing).  For the active DiD systems, the conditions in which they could be called to operate in following a DBE do not differ from their normal shutdown operation environmental conditions.  For core melt events, the **AP1000** plant DCD [2] Appendix 19D (equipment survivability assessment) evaluates the availability of equipment and instrumentation used during a severe accident to achieve a controlled, stable state after core damage under the unique containment environments. | | |
| 5.48 | 1 | The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant. | | See response for Requirement 30. | | |
| 5.49 | 1 | The qualification programme for items important for safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on items important to safety by the natural event, either by test or by analysis or by a combination of both. | | The **AP1000** plant DCD [2] Appendix 3D, Attachment B describes the **AP1000** plant Aging Evaluation Program for electric and mechanical equipment, while in Appendix 3D, Attachment C and D the effects of radiation and thermal ageing on the components is described. | | |
| 5.50 | 1 | Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme. | | See response for Requirement 30.  **AP1000** plant equipment is designed taking into consideration the environmental conditions which the component may experience during normal operation, transient and accident conditions, testing, etc. | | |
|  |  | **Requirement 31: Ageing management**  **The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.** | | The **AP1000** plant DCD [2] Appendix 3D, Attachment B describes the **AP1000** plant Aging Evaluation Program for the electrical and mechanical components, while Appendix 3D, Attachments C and D evaluated the effects of radiation and thermal ageing on the components. | | |
| 5.51 | 1 | The design for a nuclear power plant shall take due account of ageing and wear out effects in all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states in a postulated initiating event and plant states following a postulated initiating event. | | See response for Requirement 31. | | |
| 5.52 | 1 | Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help to identify unanticipated behaviour of the plant or degradation that might occur in service. | | See response for Requirement 31. | | |
|  |  | **HUMAN FACTORS** | |  | | |
|  |  | **Requirement 32: Design for optimal operator performance**  **Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.** | | The **AP1000** plant DCD [2] Section 18.2 presents the **AP1000** plant Human Factors Engineering Program Management which presents the human factors engineering program plan that is used to develop, execute, oversee, and document the human factors engineering program. This program plan includes the composition of the human factors engineering design team. | | |
| 5.53 | 1 | The design for a nuclear power plant shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state. | | The human factors design of **AP1000** plant has an established goal for minimum number of main control room (MCR) staff required to safely monitor and control the plant under all plant conditions. The plant owner will address the specific staffing levels and qualifications of plant personnel. | | |
| 5.54 | 1 | Operating personnel who have operating experience from similar plants shall, as far as is practicable, be actively involved in the design process conducted by the design organization, in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment. | | The **AP1000** plant human factors program includes involvement of experienced operators from existing PWR plants. | | |
| 5.55 | 1 | The design shall support operating personnel in the fulfillment of their responsibilities and the performance of their tasks, and shall limit the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states. | | As discussed in the **AP1000** plant DCD [2] Chapter 18, human factors engineering was implemented in the **AP1000** plant design, including a human factors engineering discipline modeling human errors. The **AP1000** plant design has been developed from the beginning taking into consideration lessons learned and input from plant operators regarding operation of plants and responsibilities for performing tasks. This includes considerations such as human performance, procedures (e.g., Technical Specifications, computerized emergency procedures, etc.) and plant layout (MCR, containment, auxiliary building) to facilitate ease of interaction between the operating personnel and the plant such that it can be operated safely and efficiently. | | |
| 5.56 | 1 | The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make a decision to act shall be simply and unambiguously presented. | | This requirement is met as discussed in the **AP1000** plant DCD [2] Section 18.4 for the Functional Requirements Analysis and Allocation, Section 18.5, Task Analysis, and other sections in Chapter 18. The task analysis provides one of the bases for the human system interface design; provides input to procedure development; provides input to staffing, training, and communications requirements of the plant; and ensures that human performance requirements do not exceed human capabilities. | | |
| 5.57 | 1 | The operator shall be provided with the necessary information:  (a) To assess the general state of the plant in any condition;  (b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions);  (c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended;  (d) To determine both the need for and the time for manual initiation of the specified safety actions. | | Displays and controls in the MCR (see **AP1000** plant DCD [2] Section 1.2.1.5.3 and Chapter 7) and plant operational procedures allow the operators to assess the general state of the plant in any conditions, operate the plant within specified limits (see **AP1000** plant DCD [2] Chapter 16) and confirm safety systems have been actuated when required and are operating as intended; These functions are met by the **AP1000** plant as discussed in:  (a) The **AP1000** plant DCD [2] Section 18.8: Human System Interface Design which presents the implementation plan for the design of the human system interface; | | |
| 5.57 (cont.) | 1 |  | | (b) & (c)  The **AP1000** plant DCD [2] Section 18.9: Procedure Development which provides input for the development of plant operating procedures, including information on the **AP1000** plant emergency response guidelines and emergency operating procedures.  (d) The **AP1000** plant post-accident monitoring requirements are specified in the **AP1000** plant DCD [2] Section 7.5. | | |
| 5.58 | 1 | The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator. | | See response for Paragraph 5.57. **AP1000** plant operating procedures have been developed taking into account considerations such as operator action time and psychological demands on the operator. | | |
| 5.59 | 1 | The need for intervention by the operator on a short time-scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and to sufficient time to act. | | This is met for the **AP1000** plant by the discussions in various sections of the **AP1000** plant DCD [2] Chapter 18.  The **AP1000** plant passive safety systems and equipment are designed to automatically establish and maintain core cooling and containment integrity for at least 72 hours following a DBE, assuming the most limiting single failure, no operator action, and no on-site and off-site ac power sources. Also see response for Paragraph 2.13. | | |
| 5.60 | 1 | The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel. | | This is met for the **AP1000** plant by the discussions in various sections of the **AP1000** plant DCD [2] including Tier 1 Sections 2.25 and 3.1; and Tier 2 Sections 1.2.1.5.3 and 1.9.2, 6.4 and Chapter 18.  The Main Control Room Emergency Habitability System (VES) is capable of maintaining the MCR environment suitable for prolonged occupancy throughout the duration of postulated accidents. See additional details in the **AP1000** plant DCD [2] Section 6.4. | | |
| 5.61 | 1 | The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts. | | The **AP1000** plant DCD Section 18.3, Operating Experience Review, discusses the process which identifies, analyzes, and addresses human factors engineering-related problems encountered in previous plant designs; and Section 18.4, Functional Requirements Analysis and Allocation, presents the results of the functional requirements analysis and function allocation process applied to the **AP1000** plant. | | |
| 5.62 | 1 | Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed. | | The **AP1000** plant DCD [2] Section 18.11 discusses meeting this requirement by the **AP1000** plant Human System Interface Verification and Validation Program. | | |
|  |  | **OTHER DESIGN CONSIDERATIONS** | |  | | |
|  |  | **Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant**  **Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.** | | This requirement is consistent with the **AP1000** plant design stand-alone unit philosophy. There is no sharing of safety systems between multiple units on a single site. | | |
| 5.63 | 1 | To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design. | | See response for Requirement 33. | | |
|  |  | **Requirement 34: Systems containing fissile material or radioactive material**  **All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as: to prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment; to prevent accidental criticality and overheating; to ensure that radioactive releases are kept below authorized limits on discharges in normal operation and below acceptable limits in accident conditions, and are kept as low as reasonably achievable; and to facilitate mitigation of radiological consequences of accidents.** | | The **AP1000** plant SSCs that provide radiation protection are described in the **AP1000** plant DCD [2] Chapters 3 through 12. Specific examples include the **AP1000** plant DCD [2] Sections 3.1, 3.5, 3.6, 3.7, 3.11.4, 4.6, 5.2, and 5.3.  Also see the responses for Requirements 5 and 78. | | |
|  |  | **Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination**  **Nuclear power plants coupled with heat utilization units (such as for district heating) and/or water desalination units shall be designed to prevent processes that transport radionuclides from the nuclear plant to the desalination unit or the district heating unit under conditions of operational states and in accident conditions.** | | This is not considered within the standard **AP1000** plant design. However, this is a well understood requirement for such eventual site specific adaptations. | | |
|  |  | **Requirement 36: Escape routes from the plant**  **A nuclear power plant shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes.** | | The **AP1000** plant DCD [2] Section 1.2, Chapter 12, and Chapter 13 provide descriptions of meeting these requirements for the **AP1000** plant.  Firefighting personnel access routes and life safety escape routes are provided for each fire area. | | |
| 5.64 | 1 | Escape routes from the nuclear power plant shall meet the relevant national and international requirements for radiation zoning and fire protection, and the relevant national requirements for industrial safety and plant security. | | Radiation zoning is described in the **AP1000** plant DCD [2] Chapter 12. Fire protection is described in the **AP1000** plant DCD [2] Section 9.5. Plant security is described in the **AP1000** plant DCD [2] Section 13.6. | | |
| 5.65 | 1 | At least one escape route shall be available from workplaces and other occupied areas following an internal event or an external event or following combinations of events considered in the design. | | See response for Requirement 36. | | |
|  |  | **Requirement 37: Communication systems at the plant**  **Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions.** | | The **AP1000** plant communication system (see **AP1000** plant DCD [2] Section 9.5.2) provides effective interplant communications and effective plant-to-offsite communications during normal, maintenance, transient, fire, and accident conditions, including loss of offsite power. | | |
| 5.66 | 1 | Suitable alarm systems and means of communication shall be provided so that all persons present at the nuclear power plant and on the site can be given warnings and instructions, in operational states and in accident conditions. | | The communication system (the **AP1000** plant DCD [2] Section 9.5.2) allows each guard, watchman, or armed response individual on duty to maintain continuous communication with an individual in each manned alarm station and with other agencies both onsite and offsite, as required by 10 CFR 73, Sections 55 (e) and (f).  The communication system consists of the following subsystems:   * Wireless telephone system * Telephone/page system * Private automatic branch exchange system * Sound-powered system * Emergency offsite communications * Security communication system.   Suitable alarm systems and means of communication are provided so that all persons present at the nuclear power plant and on the site can be given warnings and instructions, in operational states and in accident conditions. Additional details are provided in the **AP1000** plant DCD [2] Section 9.5.2. | | |
| 5.67 | 1 | Suitable and diverse means of communication necessary for safety within the nuclear power plant and in the immediate vicinity, and for communication with relevant off-site agencies, shall be provided. | | The **AP1000** plant communication system consists of the following subsystems (see **AP1000** plant DCD [2] Section 9.5.2):   * Wireless telephone system * Telephone/page system * Private automatic branch exchange system * Sound-powered system * Emergency offsite communications * Security communication system | | |
|  |  | **Requirement 38: Control of access to the plant**  **The nuclear power plant shall be isolated from its surroundings with a suitable layout of the various structural elements so that access to it can be controlled.** | | The **AP1000** plant DCD [2] Section 1.2 describes the **AP1000** plant layout that isolates the plant from its surroundings. | | |
| 5.68 | 1 | Provision shall be made in the design of the buildings and the layout of the site for the control of access to the nuclear power plant by operating personnel and/or for equipment, including emergency response personnel and vehicles, with particular consideration given to guarding against the unauthorized entry of persons and goods to the plant. | | The **AP1000** plant arrangement is as discussed in the **AP1000** plant DCD [2] Section 1.2.3. The **AP1000** plant DCD [2] Section 2.2 discusses consideration of site specific potential hazards in the licensing process. The Plant Licensee will address site-specific information related to the security of the plant. | | |
|  |  | **Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety**  **Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented.** | | The Security Plan consists of the “**AP1000** plant Physical Security Plan,” Training and Qualification Plan, and Safeguards Contingency Plan as stated in the **AP1000** plant DCD [2] Section 13.6. The Plant Licensee will address site-specific information related to the security, contingency, and guards training plans. The Plant Licensee will develop the Physical Security Plan, the Training and Qualification Plan, and the Safeguards Contingency Plan. The Plant Licensee will develop and implement a Cyber Security Program. | | |
|  |  | **Requirement 40: Prevention of harmful interactions of systems important to safety**  **The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.** | | The **AP1000** plant design was the subject of a system evaluation of potential adverse systems interactions documented in WCAP-15992, “**AP1000** Adverse Systems Interactions Evaluation Report” [18]. Interactions among I&C systems are described in the **AP1000** plant DCD [2] Chapter 7. Also see **AP1000** plant DCD [2] Section 1.9.4.2.2.A-17. | | |
| 5.69 | 1 | In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system’s operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended. | | See response for Requirement 40.  The **AP1000** plant adverse systems interactions studies document in Ref. [18] assed physical interconnections and the possible effects of one system’s operation, disoperation or malfunction on the operation of other essential systems. | | |
| 5.70 | 1 | If two fluid systems important to safety are interconnected and are operating at different pressures, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to prevent the design pressure of the system operating at the lower pressure from being exceeded. | | **AP1000** plant fluid systems design features address the potential for intersystem pressurization. For example, the normal residual heat removal system is designedto withstand the RCS pressure. | | |
|  |  | **Requirement 41: Interactions between the electrical power grid and the plant**  **The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.** | | The **AP1000** plant DCD [2] Chapter 8 discusses the connection to the utility grid and the onsite and offsite power systems for the **AP1000** plant. Note that since the passive safety systems used in the **AP1000** plant do not rely on ac power, offsite power is not important for safety. The PRA confirms this by showing extremely low risk coming from a loss of offsite power event. | | |
|  |  | **SAFETY ANALYSIS** | |  | | |
|  |  | **Requirement 42: Safety analysis of the plant design**  **A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.** | | The **AP1000** plant DCD [2] Chapters 6 and 15 detail the DBA analyses for the **AP1000** plant including the computer programs utilized. The **AP1000** plant DCD [2] Chapter 19 discusses the PRA. | | |
| 5.71 | 1 | On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed18. It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions.  *Footnote: 18 Requirements on safety assessment for facilities and activities are established in GSR Part 4 (Rev. 1) [2].* | | The safety analyses in the **AP1000** plant DCD [2] Chapters 16, 15 and 19 confirm the design of the **AP1000** plant safety design basis. | | |
| 5.72 | 1 | The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. | | The safety assessment in the **AP1000** plant DCD [2] Chapter 19 provides assurance that defense in depth measures in the **AP1000** plant design are effective and adequate. | | |
| 5.73 | 1 | The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects19 and early radioactive releases or large radioactive releases.  *Footnote: 19 A ‘cliff edge effect’, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.* | | The computer programs and their verification and validation, including treatment of uncertainties, are summarized in the **AP1000** plant DCD [2] Chapter 15 (deterministic) and Chapter 19 (PRA analyses). | | |
| 5.74 | 1 | The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design. | | Design change and as-built reconciliation procedures dictate verification of the applicability of the analytical methods.  Westinghouse has developed an initial test program, described in Chapter 14 of the AP1000 plant DCD [2] that is performed during initial startup of the AP1000 plant. The overall objective of the test program is to demonstrate that the plant has been constructed as designed, that the systems perform consistent with the plant design, and that activities culminating in operation at full licensed power including initial fuel load, initial criticality, and power ascension are performed in a controlled and safe manner. | | |
|  |  | **Deterministic approach** | |  | | |
| 5.75 | 1-7 | The deterministic safety analysis shall mainly provide:  (a) Establishment and confirmation of the design bases for all items important to safety;  (b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;  (c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements;  (d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection;  (e) Demonstration that the management of anticipated operational occurrences and design basis accident conditions is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions of the operator.  (f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator. | | The **AP1000** plant DCD [2] Chapters 6, 15, and 19 describe how these requirements are met for the **AP1000** plant DBAs. In particular:  Information related to Items (a), (b) can be found in the **AP1000** plant DCD [2] Chapter 6;  Information regarding Items (c) and (d) can be found in the **AP1000** plant DCD [2] Chapter 15;  Information regarding Items (e) and (f) can be found in the **AP1000** plant DCD [2] Chapter 19. | | |
|  |  | **Probabilistic approach** | |  | | |
| 5.76 | 1 | The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and all plant states, including shutdown, with reference in particular to:  (a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent;  (b) Providing assurance that small deviations in plant parameters that could give rise to large variations in plant conditions (cliff edge effects) will be prevented20;  (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.  *Footnote: 20 A ‘cliff edge effect’, in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.* | | The **AP1000** plant PRA summarized in the **AP1000** plant DCD [2] Chapter 19, which includes both power operation and shutdown states, was conducted with the following objectives:   * Provide an integrated view of the **AP1000** plant behavior in response to transients and accidents, including severe accidents * Satisfy the US NRC regulatory requirements that a design-specific PRA be conducted as part of the application for design certification (10 CFR 52.47(a)(i)(v)) * Demonstrate that the design meets the proposed safety goals for core damage frequency and large fission product releases * Construct a PRA Level 1 (core damage frequency), Level 2 (large release frequency), and Level 3 (offsite dose) model that is consistent with the **AP1000** plant design configuration and operation requirements and the Advanced Light Water Reactor URD requirements on PRA methodology | | |
| 5.76 (cont.) | 1 |  | | * Demonstrate the low vulnerability and insensitivity of the **AP1000** plant to human interaction * Provide input to the design process (that is, provide a tool to investigate detailed design solutions and operational strategies to optimize **AP1000** plant safety) * Demonstrate compliance with the hydrogen control criteria set forth in 10 CFR 50.34(f)(2)(ix) * Serve as a basis for an accident management program   It has also been demonstrated during the GDA process [3] that there are no cliff edge effects that may result in unforeseen risk for the safety of the plant. | | |
| **6.0** |  | **DESIGN OF SPECIFIC PLANT SYSTEMS** | |  | | |
|  |  | **REACTOR CORE AND ASSOCIATED FEATURES** | |  | | |
|  |  | **Requirement 43: Performance of fuel elements and assemblies**  **Fuel elements and assemblies for the nuclear power plant shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all processes of deterioration that could occur in operational states.** | | Fuel damage, defined as penetration of the fuel cladding, is predicted not to occur during normal operation and anticipated operational transients as discussed in the **AP1000** plant DCD [2] Section 4.1. The **AP1000** plant fuel rod and fuel assembly design bases are established to satisfy the general performance and safety criteria presented in the **AP1000** plant DCD [2] Section 4.2. The **AP1000** plant fuel rod design considers effects such as fuel density changes, fission gas release, clad creep, and other physical properties which vary with burnup. See the **AP1000** plant DCD [2] Section 4.2. | | |
| 6.1 | 1 | The processes of deterioration to be considered shall include those arising from:   * Differential expansion and deformation; * External pressure of the coolant; * Additional internal pressure due to fission products and the buildup of helium in fuel elements; * Irradiation of fuel and other materials in the fuel assembly; * Variations in pressure and temperature resulting from variations in power demand; * Chemical effects; * Static and dynamic loading, including flow induced vibrations and mechanical vibrations; * Variations in performance in relation to heat transfer that could result from distortions or chemical effects.   Allowance shall be made for uncertainties in data, in calculations and in manufacture. | | The integrity of the fuel rods is provided by designing to prevent excessive fuel temperatures as discussed in the **AP1000** plant DCD [2] Section 4.2.1.2.1; excessive internal rod gas pressures due to fission gas releases as discussed in Sections 4.2.1.3.1 and 4.2.1.3.2; and excessive cladding stresses, strains, and strain fatigue, as discussed in Sections 4.2.1.1.2 and 4.2.1.1.3. For each design basis, the performance of the limiting fuel rod, with appropriate consideration for uncertainties, does not exceed the limits specified by the design basis as discussed in the **AP1000** plant DCD [2] Section 4.2. | | |
| 6.2 | 1 | Fuel design limits shall include limits on the permissible leakage of fission products from the fuel in anticipated operational occurrences so that the fuel remains suitable for continued use. | | The mechanical design and physical arrangement of the **AP1000** plant reactor components, together with the corrective actions of the reactor control, protection, and emergency cooling systems (when applicable) are designed to achieve specified fuel design criteria as discussed in the **AP1000** plant DCD [2] Chapters 4 and 15. Fuel damage, that is, breach of fuel rod clad pressure boundary, is not expected during Condition I and Condition II events, and any small amount of fuel damage that could occur is within the capability of the plant cleanup system and is consistent with the plant design bases. See **AP1000** plant DCD [2] Section 4.2. | | |
| 6.3 | 1 | Fuel elements and fuel assemblies shall be capable of withstanding the loads and stresses associated with fuel handling. | | The **AP1000** plant fuel assemblies are designed to withstand non-operational loads induced during shipping, handling, and core loading and unloading without exceeding the criteria of the **AP1000** plant DCD [2] Section 4.2.1.5.1. | | |
|  |  | **Requirement 44: Structural capability of the reactor core**  **The fuel elements and fuel assemblies and their supporting structures for the nuclear power plant shall be designed so that, in operational states and in accident conditions other than severe accidents, a geometry that allows for adequate cooling is maintained and the insertion of control rods is not impeded.** | | The **AP1000** plant DCD [2] Section 4.2 provides the **AP1000** plant fuel system design. The plant conditions for design are divided into four categories.   * Condition I - normal operation and operational transients * Condition II - events of moderate frequency * Condition III - infrequent incidents * Condition IV - limiting faults   The core design provides adequate margin so that departure from nucleate boiling will not occur with a 95 percent probability and 95 percent confidence basis for all Condition I and II events. The reactor can be brought to a safe state following a Condition III event with only a small fraction of fuel rods damaged. The fraction of fuel rods damaged must be limited to meet the dose guidelines identified in Chapter 15 although sufficient fuel damage might occur to preclude immediate resumption of operation. The reactor can be brought to a safe state and the core kept subcritical with acceptable heat transfer geometry following transients arising from Condition IV events. | | |
|  |  | **Requirement 45: Control of the reactor core**  **Distributions of neutron flux that can arise in any state of the reactor core in the nuclear power plant, including states arising after shutdown and during or after refueling, and states arising from anticipated operational occurrences and from accident conditions not involving degradation of the reactor core, shall be inherently stable. The demands made on the control system for maintaining the shapes, levels and stability of the neutron flux within specified design limits in all operational states shall be minimized.** | | The design bases and description of **AP1000** plant nuclear design features to monitor and control neutron flux distribution are discussed in the **AP1000** plant DCD [2] Section 4.3.1.6. Limiting neutron flux (power) distributions are considered in the safety analyses (**AP1000** plant DCD [2] Chapter 15).  The core will be inherently stable to power oscillations at the fundamental mode. Spatial power oscillations within the core with a constant core power output, should they occur, can be reliably and readily detected and suppressed. The combined stability of the turbine, steam generator and the reactor power control systems are such that total core power oscillations are not normally possible. The redundancy of the protection circuits results in a low probability of exceeding design power levels. (**AP1000** plant DCD [2] Section 4.3.1.6.1 and 4.3.1.6.2) Control system operation is discussed in the **AP1000** plant DCD [2] Chapter 7. | | |
| 6.4 | 1 | Adequate means of detecting the neutron flux distributions in the reactor core and their changes shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded. | | See response for Requirement 45 and the **AP1000** plant DCD [2] Section 4.3.2.2.9 which describes the monitoring instrumentation. | | |
| 6.5 | 1 | In the design of reactivity control devices, due account shall be taken of wear out and of effects of irradiation, such as burnup, changes in physical properties and production of gas. | | The **AP1000** plant design considerations for rod cluster control assemblies and burnable absorber rods address these effects and are discussed in the **AP1000** plant DCD [2] Section 4.2.3.6. | | |
| 6.6 | 1 | The maximum degree of positive reactivity and its rate of increase by insertion in operational states and accident conditions not involving degradation of the reactor core shall be limited or compensated for to prevent any resultant failure of the pressure boundary of the reactor coolant systems, to maintain the capability for cooling and to prevent any significant damage to the reactor core. | | The maximum reactivity insertion rate is discussed in the **AP1000** plant DCD [2] Section 4.3.1.4.  The maximum reactivity insertion rate due to withdrawal of rod cluster control assemblies or gray rod cluster assemblies or by boron dilution is limited by plant design, hardware, and basic physics. During normal power operation, the maximum controlled reactivity insertion rate is limited. The maximum reactivity change rate for accidental withdrawal of two control banks is set such that peak linear heat rate and the departure from nucleate boiling ratio limitations are not challenged.  The maximum reactivity worth of control rods and the maximum rates of reactivity insertion employing control rods are limited to preclude rupture of the coolant pressure boundary or disruption of the core internals to a degree which would impair core cooling capacity due to a rod withdrawal or a postulated rod ejection accident.  Following any Condition IV occurrence, such as rod ejection or steam line break, the reactor can be brought to the shutdown condition, and the core maintains acceptable heat transfer geometry. | | |
|  |  | **Requirement 46: Reactor shutdown**  **Means shall be provided to ensure that there is a capability to shut down the reactor of the nuclear power plant in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.** | | For slowly evolving events, **AP1000** plant uses rod cluster control assemblies and chemical shim as the two diverse reactivity control systems. For fast transients, **AP1000** plant provides several additional features to supplement the chemical shim control systems. These diverse features include a diverse actuation system (DAS) which provides a different way of cutting off power to the rod cluster control assemblies (in case there is a common cause failure of the reactor trip breakers). Another diverse feature is the ability of the **AP1000** plant to “ride out” an anticipated transient event without insertion of rod cluster control assemblies using the core characteristics (such as a negative moderator coefficient) to reduce the reactor power. The DAS also supports “ride out” by actuating a turbine trip and start of the passive residual heat removal heat exchanger.  The rod cluster control assemblies and gray cluster control assemblies are inserted into the core by the force of gravity. See the **AP1000** plant DCD [2] Section 3.1 GDC 26. During operation, the shutdown rod banks are fully withdrawn. The control rod system automatically maintains a programmed average reactor temperature compensating for reactivity effects associated with scheduled and transient load changes. See the **AP1000** plant DCD [2] Section 4.3 for additional information.  The shutdown and control rod banks are designed to provide reactivity margin to shut down the reactor during normal operating conditions and during AOOs, without exceeding specified fuel design limits. | | |
|  |  | **Requirement 46: Reactor shutdown (cont.)** | | The safety analyses assume the most restrictive time in the core operating cycle and that the most reactive control rod cluster assembly is in the fully withdrawn position. See the **AP1000** plant DCD [2] Chapter 15 for summaries of the analyses, assumptions, and results. The passive safety systems provide the required boration to establish and maintain safe shutdown condition for the reactor core. See the **AP1000** plant DCD [2] Section 6.3 and the **AP1000** plant DCD [2] Section 3.1 GDC 26 for additional information.  The PMS provides the safety functions necessary to shut down the plant, and to maintain the plant in a safe shutdown condition. The PMS controls safety components in the plant that may be operated from the MCR or remote shutdown workstation.  The DAS provides a diverse means of initiating the reactor trip and emergency safety features. The PMS is designed to prevent common mode failures; however, in the low‑probability case of a common mode failure, the DAS provides diverse protection.  When fuel assemblies are in the pressure vessel and the vessel head is not in place, keff will be maintained at or below 0.95 with control rods and soluble boron. Further, the fuel will be maintained sufficiently subcritical that removal of the rod cluster control assemblies will not result in criticality. | | |
| 6.7 | 1 | The effectiveness, speed of action and shutdown margin of the means of shutdown of the reactor shall be such that the specified design limits for fuel are not exceeded. | | See response for Requirement 46. | | |
| 6.8 | 1 | In judging the adequacy of the means of shutdown of the reactor, consideration shall be given to failures arising anywhere in the plant that could render part of the means of shutdown inoperative (such as failure of a control rod to insert) or that could result in a common cause failure. | | As described in the **AP1000** plant DCD [2] Chapter 15, the **AP1000** plant design has sufficient shutdown margin even assuming that the highest worth rod cluster control assembly fails to insert.  The protection and reactivity control systems have an extremely high probability of performing their required safety functions in the event of AOOs. High quality equipment, diversity, and redundancy, support this probability. Loss of power to the protection system results in a reactor trip. Defense in depth is designed into the **AP1000** plant to reduce challenges to the protection and reactivity control systems. See the **AP1000** plant DCD [2] Section 3.1 GDC 29.  Sufficient redundancy and independence are designed into the protection systems so that no single failure or removal from service of any component or channel of a system results in loss of the protection function. Functional diversity and location diversity are designed into the system.  The diverse reactivity control system is chemical shim which for the purpose of this discussion includes the core makeup tanks. The reliability of these tanks is greater than 10‑3/demand. The DAS reliability is conservatively assumed to be 10-2 / demand (auto). | | |
| 6.9 | 1 | The means for shutting down the reactor shall consist of at least two diverse and independent systems. | | See response for Requirement 46. | | |
| 6.10 | 1 | At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core. | | The plant is provided with the means of making and maintaining the core subcritical under any anticipated condition and with appropriate margin for contingencies. Combined use of the control rod and the chemical shim control system permits the necessary shutdown margin to be maintained during long-term xenon decay and plant cooldown. The single highest worth control rod assembly is assumed to be stuck in the fully withdrawn position for this determination. See the **AP1000** plant DCD [2] Section 3.1 GDC 27. | | |
| 6.11 | 1 | The means of shutdown shall be adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality during the shutdown, or during refuelling operations or other routine or non-routine operations in the shutdown state. | | The **AP1000** plant DCD [2] Section 15.4 discusses measures to prevent unintentional reactivity insertions during shutdown conditions. | | |
| 6.12 | 1 | Instrumentation shall be provided and tests shall be specified for ensuring that the means of shutdown are always in the state stipulated for a given plant state. | | Shutdown capability and margin is controlled by Technical Specifications during plant operation, as discussed in the **AP1000** plant DCD [2] Section 16.1. | | |
|  |  | **Requirement 47: Design of reactor coolant systems**  **The components of the reactor coolant systems for the nuclear power plant shall be designed and constructed so that the risk of faults due to inadequate quality of materials, inadequate design standards, insufficient capability for inspection or inadequate quality of manufacture is minimized.** | | The **AP1000** plant reactor coolant pressure boundary components are designed, fabricated and inspected to the highest standards in accordance with the ASME Boiler and Pressure Vessel Code, Section III. See **AP1000** plant DCD [2] Section 5.2. | | |
| 6.13 | 1 | Pipework connected to the pressure boundary of the reactor coolant systems for the nuclear power plant shall be equipped with adequate isolation devices to limit any loss of radioactive fluid (primary coolant) and to prevent the loss of coolant through interfacing systems. | | The **AP1000** plant includes interconnections between high- and low-pressure systems. Each of these systems interfaces contains appropriate isolation provisions. Valves at the interface between high and low-pressure systems have redundancy to prevent low-pressure systems from being subjected to pressures that exceed their design limits.  WCAP-15993 [22] provides an evaluation of the AP1000 conformance to US NRC intersystem loss-of-coolant accident regulatory criteria.  Also see response to Requirement 48. | | |
| 6.14 | 1 | The design of the reactor coolant pressure boundary shall be such that flaws are very unlikely to be initiated, and so that any flaws that are initiated would propagate in a regime of high resistance to unstable fracture and to rapid crack propagation, thereby permitting the timely detection of flaws. | | Reactor coolant pressure boundary materials and fabrication techniques are such that there is a low probability of gross rupture or significant leakage. The **AP1000** plant RCS design incorporates pipe-break criteria (leak-before-break) to reduce or eliminate the need to consider the dynamic effects of pipe breaks. The configuration and materials of the RCS have been selected such that the pipe stresses meet the leak-before-break criteria. See the **AP1000** plant DCD [2] Section 3.6.3 for additional information. This leak-before-break design approach meets the stated requirement.  Events related to the reactor coolant system pressure boundary have also been addressed through the use of improved materials and design simplicity. For example, a reduced number of welds in the reactor coolant system piping, and the elimination of Alloy 600 in welds reduce the potential for corrosion and leakage. The reactor coolant system cold legs are single-piece bent pipe. | | |
| 6.15 | 1 | The design of the reactor coolant systems shall be such as to ensure that plant states in which components of the reactor coolant pressure boundary could exhibit embrittlement are avoided. | | The **AP1000** plant reactor coolant pressure boundary components are designed, fabricated and inspected to in accordance with the ASME Boiler and Pressure Vessel Code, Section III. See **AP1000** plant DCD [2] Section 5.2. The reactor vessel is designed to be less susceptible to brittle fracture during low temperature overpressure events. The material requirements and welding processes are developed to enhance resistance to embrittlement. | | |
| 6.16 | 1 | The design of the components contained inside the reactor coolant pressure boundary, such as pump impellers and valve parts, shall be such as to minimize the likelihood of failure and consequential damage to other components of the primary coolant system that are important to safety, in all operational states and in design basis accident conditions, with due allowance made for deterioration that might occur in service. | | The RCS components and pressure boundary is designed to accommodate the system pressures and temperatures attained under the expected modes of plant operation, including anticipated transients, while maintaining stresses within applicable limits. Components within the reactor coolant boundary are designed to minimize the likelihood of failure and consequential damage to other components of the primary coolant system that are important to safety. See **AP1000** plant DCD [2] Chapter 5.  The reactor coolant pressure boundary materials and fabrication techniques are such that there is a low probability of gross rupture or significant leakage. The **AP1000** plant RCS design incorporates pipe-break criteria (leak-before-break) that reduces the chance of a pipe rupture, improves the inspectability of the RCS pressure boundary by reducing the need for pipe whip restraints.  The configuration and materials of the RCS have been selected such that the pipe stresses meet the leak-before-break criteria. See **AP1000** plant DCD [2] Section 3.6.3 for additional information.  The reactor coolant pressure boundary and component materials are specified in the **AP1000** plant DCD [2] Chapter 5. | | |
|  |  | **Requirement 48: Overpressure protection of the reactor coolant pressure boundary**  **Provision shall be made to ensure that the operation of pressure relief devices will protect the pressure boundary of the reactor coolant systems against overpressure and will not lead to the release of radioactive material from the nuclear power plant directly to the environment.** | | Overpressure protection during power operation is provided for the RCS by the pressurizer safety valves. This protection is afforded for the following events to envelop those credible events that could lead to overpressure of the RCS if adequate overpressure protection were not provided:   * Loss of electrical load and/or turbine trip * Uncontrolled rod withdrawal at power * Loss of reactor coolant flow * Loss of normal feedwater * Loss of offsite power to the station auxiliaries   The sizing of the pressurizer safety valves is based on the analysis of a complete loss of steam flow to the turbine, with the reactor operating at 102 percent of rated power.  For those low-temperature modes of operation when operation with a water solid pressurizer is possible, a relief valve in the residual heat removal system provides low-temperature overpressure protection for the RCS.  See **AP1000** plant DCD [2] Section 5.2.2.  Lines that connect to the RCS from other systems are provided with adequate isolation as shown on the **AP1000** plant DCD [2]drawings (for example CVS in Section 9.3.6, and the normal residual heat removal system in the **AP1000** plant DCD [2] Section 5.4.7). | | |
|  |  | **Requirement 49: Inventory of reactor coolant**  **Provision shall be made for controlling the inventory, temperature and pressure of the reactor coolant to ensure that specified design limits are not exceeded in any operational states of the nuclear power plant, with due account taken of volumetric changes and leakage.** | | Changes in the reactor coolant volume will be accommodated by the pressurizer level program for normal power changes, including the transition from hot standby to full-power operation and returning to hot standby. In addition, the pressurizer has sufficient volume to accommodate minor RCS leakage.  The CVS is normally used to maintain the required coolant inventory in the RCS and maintains the programmed pressurizer water level during normal plant operations. See **AP1000** plant DCD [2] Section 9.3.6.  Safety passive RCS makeup is provided to maintain the RCS inventory in case the CVS is unavailable. It can accommodate small leaks when the normal CVS makeup system is unavailable and can accommodate larger leaks resulting LOCAs. Safety reactor coolant makeup and safety injection are provided by the passive core cooling system described in the **AP1000** plant DCD [2] Section 6.3.  Provisions are made for detection of leakage through the reactor coolant boundary for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Section 5.2.5. | | |
|  |  | **Requirement 50: Cleanup of reactor coolant**  **Adequate facilities shall be provided at the nuclear power plant for the removal from the reactor coolant of radioactive substances, including activated corrosion products and fission products deriving from the fuel, and non-radioactive substances.** | | The CVS maintains RCS fluid purity and activity level within acceptable limits. See the **AP1000** plant DCD [2] Section 9.3.6. | | |
| 6.17 | 1 | The capabilities of the necessary plant systems shall be based on the specified design limit on permissible leakage for the fuel, with a conservative margin to ensure that the plant can be operated with a level of circuit activity that is as low as reasonably practicable, and to ensure that the requirements are met for radioactive releases to be as low as reasonably achievable and below the authorized limits on discharges. | | The CVS (**AP1000** plant DCD [2] Section 9.3.6.1.2.1) is designed to maintain the RCS activity level at less than the technical specification limit for normal operations, with design basis fuel defects. The technical specifications allow these limits to be exceeded for a specified duration. See **AP1000** plant DCD [2] Chapter 16.  The CVS purification capability considers occupational radiation exposure to support ALARA goals. (**AP1000** plant DCD [2] Section 9.3.6.1.2) | | |
|  |  | **Requirement 51: Removal of residual heat from the reactor core**  **Means shall be provided for the removal of residual heat from the reactor core in the shutdown state of the nuclear power plant such that the design limits for fuel, the reactor coolant pressure boundary and structures important to safety are not exceeded.** | | The **AP1000** plant design satisfies this requirement through the use of redundant and diverse sets of decay heat removal systems. These systems reduce the risk associated with loss of the decay heat removal function through a combination of passive safety systems, together with the active DiD systems. Specific decay heat removal systems include the following (**AP1000** plant DCD [2] Section 9.3):   * A safety passive residual heat removal heat exchanger that uses natural circulation flow, and can operate at high RCS pressure, and that does not require electrical power for operation * Automatic, passive safety feed and bleed using the core makeup tanks, accumulators, and the in-containment refueling water storage tank for injection and the automatic depressurization system valves for RCS venting * The DiD startup feedwater system with motor-driven pumps supplied by offsite or onsite power, including automatic sequencing on the DiD diesel generators * The DiD normal residual heat removal system with motor-driven pumps supplied by offsite or onsite power, including DiD diesel generators, for use at low RCS pressures. | | |
|  |  | **Requirement 52: Emergency cooling of the reactor core**  **Means of cooling the reactor core shall be provided to restore and maintain cooling of the fuel under accident conditions at the nuclear power plant even if the integrity of the pressure boundary of the primary coolant system is not maintained.** | | The **AP1000** plant design provides for safety passive high pressure injection into the RCS. The Core Makeup (**AP1000** plant PRA [4] Chapter 9, **AP1000** plant DCD [2] Section 6.3) Tanks provide this capability. Accumulators provide the high initial injection flow required for a large LOCA and initiate injection when the RCS pressure decreases below the static accumulator pressure.  The in-containment refueling water storage tank and containment recirculation capability provide the long-term source of injection to the core after the RCS is depressurized. The automatic depressurization system reduces the RCS pressure such that the in-containment refueling water storage tank can inject by gravity head and containment recirculation can occur by natural circulation.  The passive core cooling system is discussed in the **AP1000** plant DCD [2] Section 6.3. | | |
| 6.18 | 1-5 | The means provided for cooling of the reactor core shall be such as to ensure that:  (a) The limiting parameters for the cladding or for integrity of the fuel (such as temperature) will not be exceeded;  (b) Possible chemical reactions are kept to an acceptable level;  (c) The effectiveness of the means of cooling of the reactor core compensates for possible changes in the fuel and in the internal geometry of the reactor core;  (d) Cooling of the reactor core will be ensured for a sufficient time. | | The safety analyses for LOCA are discussed in the **AP1000** plant DCD [2] Section 15.6 and show that specified LOCA criteria are met. | | |
| 6.19 | 1 | Design features (such as leak detection systems, appropriate interconnections and capabilities for isolation) and suitable redundancy and diversity shall be provided to fulfil the requirements of para. 6.18 with adequate reliability for each postulated initiating event. | | The **AP1000** plant design provides a passive core cooling system that functions independent of ac power supplies, and assuming single active failures. It has component redundancy to provide confidence that its safety functions are performed, even in the unlikely event of the most limiting single failure occurring coincident with postulated DBEs. It is designed to be sufficiently reliable, considering redundancy and diversity, to support the plant core melt frequency and large release frequency goals.  Leak detection is discussed in the **AP1000** plant DCD [2] Chapter 3 Appendix 3B.  Also see response for Paragraph 6.13 regarding isolation capabilities of systems connected to the RCS. | | |
|  |  | **Requirement 53: Heat transfer to an ultimate heat sink**  **The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.** | | The **AP1000** plant passive containment cooling system passively transfers decay heat from inside the containment to the atmosphere, which is the ultimate heat sink for accident conditions (refer to the **AP1000** plant DCD [2] Section 6.2.2). The passive containment cooling system does not rely upon offsite or onsite ac power sources. Heat transfer occurs by convection and water evaporation from the containment shell to the atmosphere. The water is stored inside a tank located above the containment vessel and drains by gravity when initiated. This water flow is initiated by opening only one of three valves. These valves provide a highly reliable (redundant and diverse) means of initiating this water flow. Additional information is provided in the **AP1000** plant DCD [2] Section 3.1 responses for GDC 34 and GDC 38. | | |
| 6.19A | 1 | Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink. | | The passive containment cooling system design is highly robust, and makes use of redundancy, diversity and fail-safe measures, which do not require any support system to operate. Furthermore, air-only cooling provides long grace period for the operator to establish water cooling following an event. See [14]. | | |
| 6.19B | 1 | The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site. | | The AP1000 plant meets this requirement as described in [14], [16] and in Appendix 12B of the **AP1000** plant PCSR [19]. | | |
|  |  | **CONTAINMENT STRUCTURE AND CONTAINMENT SYSTEM** | |  | | |
|  |  | **Requirement 54: Containment system for the reactor**  **A containment system shall be provided to ensure, or to contribute to, the fulfilment of the following safety functions at the nuclear power plant: (i) confinement of radioactive substances in operational states and in accident conditions, (ii) protection of the reactor against natural external events and human induced events and (iii) radiation shielding in operational states and in accident conditions.** | | The **AP1000** plant containment system is described in the **AP1000** plant DCD [2] Section 6.2. The containment consists of a steel containment vessel and is surrounded by a concrete shield building. The containment is designed to house the RCS and other safety systems. The containment vessel functions as an essentially leaktight barrier. In addition, the steel containment performs passive core cooling functions as part of the passive containment cooling system to transfer heat from containment to the ultimate heat sink (the atmosphere). It is protected against malevolent aircraft impact, environmental hazards (e.g., flooding) and postulated missiles from external sources (by the shield building) as well as missiles produced by internal equipment failures.  Containment hydrogen control is discussed in the **AP1000** plant DCD [2] Section 6.2.4.  Containment penetrations are isolated according to the provisions of US NRC GDCs 54, 55, 56, and 57 as presented in the **AP1000** plant DCD [2] Section 3.1. Containment isolation is discussed in the **AP1000** plant DCD [2] Section 6.2.3. | | |
|  |  | **Requirement 55: Control of radioactive releases from the containment The design of the containment shall be such as to ensure that any release of radioactive material from the nuclear power plant to the environment is as low as reasonably achievable, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions.** | | The **AP1000** plant containment systems are described in the **AP1000** plant DCD [2] Section 6.2. The safety analyses (**AP1000** plant DCD [2] Chapters 15 and 19) show that release of radioactive material from the nuclear power plant to the environment is ALARA, is below the authorized limits on discharges in operational states and is below acceptable limits in accident conditions. | | |
| 6.20 | 1 | The containment structure and the systems and components affecting the leaktightness of the containment system shall be designed and constructed so that the leak rate can be tested after all penetrations through the containment have been installed and, if necessary during the operating lifetime of the plant, so that the leak rate can be tested at the containment design pressure. | | The **AP1000** plant containment leak rate test system provides this capability as described in the **AP1000** plant DCD [2] Section 6.2.5. | | |
| 6.21 | 1 | The number of penetrations through the containment shall be kept to a practical minimum and all penetrations shall meet the same design requirements as the containment structure itself. The penetrations shall be protected against reaction forces caused by pipe movement or accidental loads such as those due to missiles caused by external or internal events, jet forces and pipe whip. | | The number of penetrations through the **AP1000** plant containment has been reduced as a result of the use of passive safety systems and other plant simplifications. Most penetrations are normally closed, and all penetrations use remotely operated valves for isolation that close automatically. Where possible, the containment isolation valves are fail-closed air operated valves which fail to their safe position on a loss of power, loss of signal, or loss of air. See **AP1000** plant DCD [2] Section 6.2.3 for additional information.  Piping systems penetrating the containment have containment isolation features. These features serve to minimize the release of fission products following a DBA. Standard Review Plan Section 6.2.4 provides acceptable alternative arrangements to the explicit arrangements given in US NRC GDC 55, 56 and 57. **AP1000** plant DCD [2] Table 6.2.3-1 lists each penetration and provides a summary of the containment isolation characteristics. The Piping and Instrumentation Diagrams of the applicable systems show the functional arrangement of the containment penetration, isolation valves, test and drain connections.  The safety classification of the containment penetrations are the same as the containment itself (**AP1000** plant Safety Class B, Seismic Category 1). Also refer to the **AP1000** plant DCD [2] Section 6.2.3 and response for Paragraph 6.13. | | |
|  |  | **Requirement 56: Isolation of the containment**  **Each line that penetrates the containment at a nuclear power plant as part of the reactor coolant pressure boundary or that is connected directly to the containment atmosphere shall be automatically and reliably sealable in the event of an accident in which the leaktightness of the containment is essential to preventing radioactive releases to the environment that exceed acceptable limits.** | | The **AP1000** plant containment isolation provides two barriers -- one inside containment and the other outside containment. See **AP1000** plant DCD [2] Section 1.9. Testing connections are provided to facilitate leak testing of the penetrations and their isolation valves.  Containment isolation is automatically actuated by a safeguards actuation signal, using two-out-of-four coincident logic. The containment isolation actuation is set as low as reasonable without creating potential for spurious trips during normal operations. Containment isolation can also be initiated manually from the MCR. Containment penetrations do not automatically reopen on the resetting of the isolation signal. See subsection 6.2.3 for additional information.  The DAS provides a backup means of actuating risk important containment penetrations. | | |
| 6.22 | 1 | Lines that penetrate the containment as part of the reactor coolant pressure boundary and lines that are connected directly to the containment atmosphere shall be fitted with at least two adequate containment isolation valves or check valves arranged in series21 and shall be provided with suitable leak detection systems. Containment isolation valves or check valves shall be located as close to the containment as is practicable, and each valve shall be capable of reliable and independent actuation and of being periodically tested.  *Footnote: 21 In most cases, one containment isolation valve or check valve is outside the containment and the other is inside the containment. Other arrangements might be acceptable, however, depending on the design.* | | The **AP1000** plant design meets these containment isolation requirements. Refer to the **AP1000** plant DCD [2] Section 3.1.1 - Criterion 55 – Reactor Coolant Pressure Boundary Penetrating Containment and the **AP1000** plant DCD [2] Section 6.2.3.  Also see response for Requirement 56 and Paragraphs 6.13 and 6.21. | | |
| 6.23 | 1 | Exceptions to the requirements for containment isolation in para. 6.22 shall be permissible for specific classes of lines such as instrumentation lines, or in cases in which application of the methods of containment isolation specified in para. 6.22 would reduce the reliability of a safety system that includes a penetration of the containment. | | See response for Requirement 6.22.  Exception may be constituted by instrumentation lines (see **AP1000** plant DCD [2] Section 6.2.3.1.1 Point G). | | |
| 6.24 | 1 | Each line that penetrates the containment and is neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall have at least one adequate containment isolation valve. The containment isolation valves shall be located outside the containment and as close to the containment as is practicable. | | Each line that penetrates the containment, that is neither part of the reactor coolant pressure boundary nor connected directly to the atmosphere of the containment, and that satisfies the requirements of a closed system is provided with a containment isolation valve according to US NRC GDC 57. A closed system is not a part of the reactor coolant pressure boundary and is not connected directly to the atmosphere of the containment. See **AP1000** plant DCD [2] Section 6.2.1.1.1 for additional details.  Each line that penetrates the containment that either connects to the RCS or that connects directly to the containment atmosphere, and does not meet the requirements for a closed system (as defined below), is provided with containment isolation valves according to US NRC GDC 55 and 56. | | |
|  |  | **Requirement 57: Access to the containment**  **Access by operating personnel to the containment at a nuclear power plant shall be through airlocks equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions.** | | Two personnel airlocks are provided; one located adjacent to each of the equipment hatches, and equipped with doors that are interlocked to ensure that at least one of the doors is closed during reactor power operation and in accident conditions. **AP1000** plant DCD [2] Figure 3.8.2-3 shows the typical arrangement. Refer to the **AP1000** plant DCD [2] Section 3.8.2. | | |
| 6.25 | 1 | Where provision is made for entry of operating personnel for surveillance purposes, provisions for ensuring protection and safety for operating personnel shall be specified in the design. Where equipment air locks are provided, provisions for ensuring protection and safety for operating personnel shall be specified in the design. | | Access control provisions for safety of personnel are described in the **AP1000** plant DCD [2] Chapter 12. | | |
| 6.26 | 1 | Containment openings for the movement of equipment or material through the containment shall be designed to be closed quickly and reliably in the event that isolation of the containment is required. | | Closure of the containment equipment hatch is a standard design capability for the **AP1000** plant, as reflected in NUREG-1431, Technical Specification 3.9.4 (see **AP1000** plant DCD [2] Chapter 16) for containment penetrations.  The equipment hatch is closed and held in place by [four] bolts, during movement of recently irradiated fuel assemblies within containment. The need for equipment hatch closure during refueling, as discussed in the Bases for TS 3.9.4, is based on a fuel handling accident with a dropped fuel assembly.  Current plants also have a requirement to be able to close the equipment hatch on [four] bolts within 4 hours of the loss of residual heat removal cooling while flooded up in the refueling cavity for refueling operations.  The **AP1000** plant design has safety analyses for radioactive dose that allows this to be modified for a fuel handling accident, and the concern for the **AP1000** plant design is now a loss of the passive safety system cooling water inventory during a loss of decay heat removal event, out of containment penetrations once steam formation occurs. | | |
| 6.26 (cont.) | 1 |  | | Thus, the equivalent **AP1000** plant Technical Specification 3.6.8 (**AP1000** plant DCD [2] Chapter 16) has been modified as follows: “a. The equipment hatches closed and held in place by four bolts or, if open, clear of obstructions such that the hatches can be closed prior to steaming into the containment” during Mode 5 or 6. During fuel handling operations, Technical Specification 3.9.5 requires either the equipment hatch closed and held in place with 4 bolts, or if it is open, then the containment air filtration system must be operating.  Each of the two equipment hatches is provided with an electrically powered hoist and with a set of hardware, tools, equipment and has a self-contained power source for moving the hatch from its storage position if ac electrical power is not available. Refer to the **AP1000** plant DCD [2] Section 3.8.2. | | |
|  |  | **Requirement 58: Control of containment conditions**  **Provision shall be made to control the pressure and temperature in the containment at a nuclear power plant and to control any buildup of fission products or other gaseous, liquid or solid substances that might be released inside the containment and that could affect the operation of systems important to safety.** | | The containment recirculation cooling system (see **AP1000** plant DCD [2] Section 9.4.6) controls building air temperature and humidity to provide a suitable environment for equipment operability during normal operation and shutdown.  The containment air filtration system (see **AP1000** plant DCD [2] Section 9.4.7) provides the following functions: | | |
|  |  | **Requirement 58: Control of containment conditions (cont.)** | | * Provides intermittent flow of outdoor air to purge the containment atmosphere of airborne radioactivity during normal plant operation, and continuous flow during hot or cold plant shutdown conditions to provide an acceptable airborne radioactivity level prior to and during personnel access * Provides intermittent venting of air into and out of the containment to maintain the containment pressure within its design pressure range during normal plant operation * Directs the exhaust air from the containment atmosphere to the plant vent for monitoring, and provides filtration to limit the release of airborne radioactivity at the site boundary within acceptable levels * Monitors gaseous, particulate and iodine concentration levels discharged to the environment through the plant vent   The **AP1000** plant is designed with in-containment leakage collection and with adequate drains and sump with redundant sump pumps to prevent accumulation of liquids within containment. Refer to the **AP1000** plant DCD [2] Chapter 11.  The **AP1000** plant DCD [2] Section 3.11 describes the environmental qualification of equipment. | | |
| 6.27 | 1 | The design shall provide for sufficient flow routes between separate compartments inside the containment. The cross-sections of openings between compartments shall be of such dimensions as to ensure that the pressure differentials occurring during pressure equalization in accident conditions do not result in unacceptable damage to the pressure bearing structure or to systems that are important in mitigating the effects of accident conditions. | | Containment structures are arranged to promote mixing via natural circulation. The physical mechanisms of natural circulation mixing that occur in the **AP1000** plant are discussed in the **AP1000** plant DCD [2] Appendix 6A.  Per the **AP1000** plant DCD [2] Section 6.2.1.1, subcompartments within containment are designed to withstand the transient differential pressures of a postulated pipe break. These subcompartments are vented so that differential pressures remain within structural limits. The subcompartment walls are challenged by the differential pressures resulting from a break in a high energy line. Therefore, a high energy line is postulated, with a break size chosen consistent with the position presented in the **AP1000** plant DCD [2] Section 3.6, for analyzing the maximum differential pressures across subcompartment walls. | | |
| 6.28 | 1 | The capability to remove heat from the containment shall be ensured, in order to reduce the pressure and temperature in the containment, and to maintain them at acceptably low levels, after any accidental release of high energy fluids. The systems performing the function of removal of heat from the containment shall have sufficient reliability and redundancy to ensure that this function can be fulfilled. | | The **AP1000** plant passive containment cooling provides passive decay heat removal that transfers heat to the atmosphere, which is the ultimate heat sink for accident conditions. The passive containment cooling system utilizes the steel containment vessel to transfer heat from inside the containment to the atmosphere and is designed with both redundant and diverse means of actuation to maximize reliability to ensure that this function can be fulfilled (refer to the **AP1000** plant DCD [2] Section 6.2.2). | | |
| 6.28A | 1 | Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release. | | The passive containment cooling system design is highly robust, and makes use of redundancy, diversity and fail-safe measures, which do not require any support system to operate. Furthermore, air-only cooling provides long grace period for the operator to establish water cooling following an event. See [14].  Containment integrity is also provided for core melt event is demonstrated in the PRA (Chapter 19 of the **AP1000** plant DCD [2]). | | |
| 6.28B | 1 | The design shall also include features to enable the safe use of non-permanent equipment22 for restoring the capability to remove heat from the containment.  *Footnote: 22 Non-permanent equipment need not necessarily be stored on the site.* | | The **AP1000** plant design includes safety connections available for the connection of non-permanent equipment as discussed in [14] and in Appendix 12B of the **AP1000** plant PCSR [19]. | | |
| 6.29 | 1 | Design features to control fission products, hydrogen, oxygen and other substances that might be released into the containment shall be provided as necessary:  (a) To reduce the amounts of fission products that could be released to the environment in accident conditions;  (b) To control the concentrations of hydrogen, oxygen and other substances in the containment atmosphere in accident conditions so as to prevent deflagration or detonation loads that could challenge the integrity of the containment. | | During normal operation, the CVS controls/maintains the primary coolant water chemistry and fission product concentrations inside Technical Specification values. This assures that should a LOCA occur the fission products, hydrogen, oxygen and other substances that might be released into containment are within the assumptions taken in the plant licensing analyses.  During an accident, fission product control for the **AP1000** plant is provided via natural removal processes within containment and by limiting containment leakage. The passive removal processes such as deposition and sedimentation are evaluated based on a physically-based source term with large scale core damage. See the **AP1000** plant DCD [2] Section 6.5 and Appendix 15B for additional details.  The containment and penetration design includes features specifically designed to minimize overall containment leakage. See subsection 6.2.3 for additional details. | | |
| 6.29 (cont.) | 1 |  | | Hydrogen control is provided as described in the **AP1000** plant DCD [2] Section 3.1, GDC 41. The generation of hydrogen in the containment under post-accident conditions has been evaluated, and the containment hydrogen control system has been designed such that the following criteria are satisfied:   * In compliance with Section 50.44 of 10 CFR 50, means are provided to measure and control post-LOCA hydrogen concentrations. * The combustible concentrations of hydrogen do not accumulate in the areas where unintended combustion or detonation could cause loss of containment integrity or loss of appropriate mitigating features. * Internal passive autocatalytic recombiners are provided for hydrogen control following a design basis LOCA. * Hydrogen igniters are provided to limit local and global hydrogen concentrations to below 10 percent following a degraded core event with the reaction of 100 percent of the zircaloy cladding. | | |
| 6.29 (cont.) | 1 |  | | * The concentration of uniformly distributed hydrogen produced by the equivalent of a 75 percent active fuel-clad metal water reaction does not exceed 13 percent by volume during and following a degraded core event. (The **AP1000** plant containment volume is large enough to provide passive protection for the hydrogen produced by 75 percent zircaloy cladding reaction following a severe accident.). Should a deflagration occur no containment failure is predicted as consequence of the event, assuming best estimate/realistic approach (see **AP1000** plant DCD [2] Chapter 19, Section 19.41.12 Summary) * The non-safety ventilation system, normally used during refueling, is designed with the capability for a controlled purge of the containment atmosphere to assist in post-accident cleanup, but is not required for hydrogen control. | | |
| 6.30 | 1 | Coverings, thermal insulations and coatings for components and structures within the containment system shall be carefully selected and methods for their application shall be specified to ensure the fulfilment of their safety functions and to minimize interference with other safety functions in the event of deterioration of the coverings, thermal insulations and coatings. | | Per the **AP1000** plant DCD [2] Section 6.3.2.4, a qualified, corrosion-resistant paint or coating is specified to enhance surface wetability and water film formation for the portion of the containment vessel that transfers heat to the environment. Other coatings used inside the containment are qualified but are not required to be safety because they have a high density and will settle out of the recirculation flow following an accident.  Additional design considerations addressing screens that provide the long term, recirculation, emergency core cooling flowpaths are described in the **AP1000** plant DCD [2] Section 6.3.2.2.7. | | |
|  |  | **INSTRUMENTATION AND CONTROL SYSTEMS** | |  | | |
|  |  | **Requirement 59: Provision of instrumentation**  **Instrumentation shall be provided for: determining the values of all the main variables that can affect the fission process, the integrity of the reactor core, the reactor coolant systems and the containment at the nuclear power plant; for obtaining essential information on the plant that is necessary for its safe and reliable operation; for determining the status of the plant in accident conditions; and for making decisions for the purposes of accident management.** | | The **AP1000** plant I&C systems meet these requirements by providing protection against unsafe reactor operation. The **AP1000** plant DCD [2] Chapter 7, “Instrumentation and Controls” discusses the architecture of the **AP1000** plant I&C systems, including the **AP1000** plant PLS and the PMS, and other systems. | | |
| 6.31 | 1 | Instrumentation and recording equipment shall be provided to ensure that essential information is available for monitoring the status of essential equipment and the course of accidents, for predicting the locations of release and amount of radioactive material that could be released from the locations that are so intended in the design, and for post-accident analysis. | | The PMS is the aggregate of electrical and mechanical equipment which senses generating station conditions and generates the signals to actuate reactor trip and engineered safety features functions, and which provides the equipment necessary to monitor plant safety functions during and following designated events as required by Regulatory Guide 1.97. See **AP1000** plant DCD [2] Sections 7.1.2 and 7.5. | | |
|  |  | **Requirement 60: Control systems**  **Appropriate and reliable control systems shall be provided at the nuclear power plant to maintain and limit the relevant process variables within the specified operational ranges.** | | The PLS provides the functions necessary for normal operation of the plant from cold shutdown through full power operation. The PLS controls non-safety and DiD components in the plant that are operated from the MCR or remote shutdown workstation. The PLS is described in the **AP1000** plant DCD [2] Sections 7.1.3 and 7.7.1. | | |
|  |  | **Requirement 61: Protection system**  **A protection system shall be provided at the nuclear power plant that has the capability to detect unsafe plant conditions and to initiate safety actions automatically to actuate the safety systems necessary for achieving and maintaining safe plant conditions.** | | The **AP1000** plant PMS is discussed in DCD Sections 7.1.2, 7.2 and 7.3. The deterministic safety analyses in the **AP1000** plant DCD [2] Chapter 15 show that these requirements are met. In addition, see response for Paragraph 6.32. | | |
| 6.32 | 1-3 | The protection system shall be designed:  (a) To be capable of overriding unsafe actions of the control system;  (b) With fail-safe characteristics to achieve safe plant conditions in the event of failure of the protection system. | | See response for Requirement 61.  The control system overrides unsafe actions of the control systems (e.g., Rod control system - rod withdrawal) – See also **AP1000** plant DCD [2] Section 7.6 Interlock Systems Important to Safety.  The control system is designed with a 2-out-of-4 logic. It can work with one channel out of service or in maintenance and still maintain a 2-out-of-3 logic to avoid spurious actuations.  A failure modes and effects analysis was performed on the **AP1000** plant PMS. Through the process of examining the feasible failure modes, it was concluded that the **AP1000** plant PMS maintains safety functions during single point failures. The **AP1000** plant failure modes and effects analysis is documented in Reference 1. The Common Q failure modes and effects analysis is documented in Reference 3 and also concludes that the protection system maintains safety functions during single point failures. (See **AP1000** plant DCD [2] Section 7.2.2.1). One channel of the protection system can be bypassed for an indefinite period of time with the normal two-out-of-four trip logic automatically reverting to a two-out-of-three trip logic. Bypassing two or more channels is not allowed. | | |
| 6.32 (cont.) | 1 |  | | In case of complete failure of the protection system the plant can be brought to a safe condition by the DAS. The DAS is a DiD, diverse system that provides an alternate means of initiating reactor trip and actuating selected engineered safety features, and providing plant information to the operator. The DAS is described in the **AP1000** plant DCD [2] Section 7.7.1.11. | | |
| 6.33 | 1 | The design:  (a) Shall prevent operator actions that could compromise the effectiveness of the protection system in operational states and in accident conditions, but shall not counteract correct operator actions in accident conditions;  (b) Shall automate various safety actions to actuate safety systems so that operator action is not necessary within a justified period of time from the onset of anticipated operational occurrences or accident conditions;  (c) Shall make relevant information available to the operator for monitoring the effects of automatic actions. | | See response for Requirement 61and Paragraph 6.32.  The PMS design includes the following features:   1. The PMS is designed so that operator cannot compromise its effectiveness. For example, each channel used in reactor trip can be bypassed, as discussed in the **AP1000** plant DCD [2] Section 7.1.2.9, except for reactor trips resulting from manual initiations. One channel can be bypassed for an indefinite period of time with the normal two-out-of-four trip logic automatically reverting to a two-out-of-three trip logic. Bypassing two or more channels is not allowed. 2. The PMS and passive safety systems are designed such that operator actions are not required for 72 hours following a DBE. | | |
| 6.33 (cont.) | 1 |  | | 1. An analysis is conducted to identify the appropriate variables and to establish the appropriate design bases and qualification criteria for instrumentation employed by the operator for monitoring conditions in the RCS, the secondary heat removal system, the containment, and the systems used for attaining a safe shutdown condition. This selection of monitored variables is based on the guidance provided in Regulatory Guide 1.97. The variables and instrument design criterion selected for the **AP1000** plant is described in the **AP1000** plant DCD [2] Sections 7.5.2 and 7.5.3. (Also see **AP1000** plant DCD [2] Section 7.5 “Safety‑Related Display Information”.) | | |
|  |  | **Requirement 62: Reliability and testability of instrumentation and control systems**  **Instrumentation and control systems for items important to safety at the nuclear power plant shall be designed for high functional reliability and periodic testability commensurate with the safety function(s) to be performed.** | | The PMS consists of four redundant divisions, designated A, B, C, and D. The PMS performs the necessary safety signal acquisition, calculations, setpoint comparison, coincidence logic (2 out of 4), reactor trip/ engineered safety features actuation functions, and component control functions to achieve and maintain the plant in a safe shutdown condition. The PMS also contains maintenance and test functions to verify proper operation of the system. The PMS includes four redundant safety displays, one for each division, located on the primary dedicated safety panel in the MCR. Four redundant divisions are provided to satisfy single failure criteria and improve plant availability.  The I&C equipment performing reactor trip and engineered safety features actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic.  The PMS is described in the **AP1000** plant DCD [2] Chapter 7.  Additional information may be found in Reference 5: Section 7 describes the fault tolerance features, and Section 6 describes the maintenance, test, and bypass features of the PMS. | | |
| 6.34 | 1 | Design techniques such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity and diversity in component design and concepts of operation shall be used to the extent practicable to prevent loss of a safety function. | | These design techniques are used extensively in the design of the **AP1000** plant protection systems. For example, a single failure in the PMS or the reactor trip actuation divisions does not prevent a reactor trip, even when a reactor trip channel is bypassed for test or maintenance. In addition to the redundancy of equipment, diversity of reactor trip functions is incorporated. For example, reactor trip, because of an uncontrolled rod cluster control assembly bank withdrawal at power, may occur on power range high neutron flux, overtemperature, overpower, pressurizer high pressure or pressurizer high water level. Reactor trip on complete loss of reactor coolant flow may occur on low flow or from the diverse parameter of low reactor coolant pump speed.  Common mode failures are considered in the PRA. The **AP1000** plant DAS provides defense‑in‑depth in the event of complete failure of the protection system. | | |
| 6.35 | 1 | Safety systems shall be designed to permit periodic testing of their functionality when the plant is in operation, including the possibility of testing channels independently for the detection of failures and losses of redundancy. The design shall permit all aspects of functionality testing for the sensor, the input signal, the final actuator and the display. | | The **AP1000** plant PMS is based on a 2 out of 4 architecture.  One channel of the protection system can be bypassed for an indefinite period of time with the normal two-out-of-four trip logic automatically reverting to a two-out-of-three trip logic. Bypassing two or more channels is not allowed.  During testing/maintenance single channel are bypassed reverting to a two-out-of-three trip logic and still maintaining a high degree of robustness against spurious signals.  Maintenance and testing of the PMS consists of two types of tests: self-diagnostic tests and on-line verification tests. The self-diagnostic tests consist of numerous automatic checks to validate that the equipment and software are performing their functions correctly. On-line verification tests are manually initiated to verify that the safety system is capable of performing its intended safety function.  During operation of the reactor, the engineered safety features final actuators, whose operation is compatible with continued plant operation, are tested periodically. Continuity of the wiring is verified for devices that cannot be tested at power without damaging or upsetting the plant, operability of the final actuated equipment is demonstrated at shutdown.  Also see **AP1000** plant DCD [2] Chapter 7 and Reference [5]. | | |
| 6.36 | 1 | When a safety system, or part of a safety system, has to be taken out of service for testing, adequate provision shall be made for the clear indication of any protection system bypasses that are necessary for the duration of the testing or maintenance activities. | | See response for Requirement 62.  The issue of safety systems or equipment out of service is also addressed in the plant Technical Specifications (**AP1000** plant DCD [2] Chapter 16). | | |
|  |  | **Requirement 63: Use of computer based equipment in safety systems important to safety**  **If a system important to safety at the nuclear power plant is dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle. The entire development shall be subject to a quality management system.** | | The **AP1000** plant meets these requirements as discussed in the **AP1000** plant DCD [2] Chapter 7. Also a planned design process has been established for software development during life cycle stages. This process includes a thorough verification and validation process to be applied to the safety related software. Approved methods are established for the use of commercial off-the-shelf hardware and software through a commercial dedication process.  In addition, the **AP1000** plant design includes the DAS which provides a diverse means of actuating the passive safety features. | | |
| 6.37 | 1-7 | For computer based equipment in safety systems or safety related systems:  (a) A high quality of, and best practices for, hardware and software shall be used, in accordance with the importance of the system to safety.  (b) The entire development process, including control, testing and commissioning of design changes, shall be systematically documented and shall be reviewable.  (c) An assessment of the equipment shall be undertaken by experts who are independent of the design team and the supplier team to provide assurance of its high reliability.  (d) Where safety functions are essential for achieving and maintaining safe conditions, and the necessary high reliability of the equipment cannot be demonstrated with a high level of confidence, diverse means of ensuring the fulfilment of the safety functions shall be provided.  (e) Common cause failures deriving from software shall be taken into consideration.  (f) Protection shall be provided against accidental disruption of, or deliberate interference with, system operation. | | See response to Requirement 63.   1. The PMS is a safety related system. It’s designed and fabricated according to Institute of Electrical and Electronic Engineers (IEEE) standards including IEEE-323-1983 & IEEE-344-1987. 2. The PMS a safety system. Subject to 10CFR21, 10CFR50 Appendix B, US NRC Group C. 3. Reviews have been performed by independent safety authorities in US, China and the UK. 4. The **AP1000** plant design uses passive safety systems that are highly reliable as demonstrated by the PSA evaluations. Once actuated they do not require ac power or support systems. In addition safety systems actuation can also be actuated by the DAS should the PMS be unavailable. 5. Common causes failures are taken into consideration (see **AP1000** plant DCD [2] Sections 7.2.2.1 and 7.3.2.1) 6. Protection is provided against accidental disruption or deliberate interference with system operation. | | |
|  |  | **Requirement 64: Separation of protection systems and control systems**  **Interference between protection systems and control systems at the nuclear power plant shall be prevented by means of separation, by avoiding interconnections or by suitable functional independence.** | | Per the **AP1000** plant DCD [2] Section 3.1, conformance with US NRC GDC 24, the protection system is separate and distinct from the control systems. Control systems are, in some cases, dependent on the protection system for signals that are derived from protection system measurements, where applicable. These signals are transferred to the control system by isolation devices classified as protection components. The adequacy of the system isolation is verified by testing under conditions of postulated credible faults. The failure of a single control system component or channel, or the failure or removal from service of a single protection system component or channel common to the control and protection system, leaves intact a system that satisfies the requirements of the protection system. The removal of a protection division from service is allowed during testing of the division. | | |
| 6.38 | 1 | If signals are used in common by both a protection system and any control system, separation (such as by adequate decoupling) shall be ensured and the signal system shall be classified as part of the protection system. | | See response for Requirement 64. | | |
|  |  | **Requirement 65: Control room**  **A control room shall be provided at the nuclear power plant from which the plant can be safely operated in all operational states, either automatically or manually, and from which measures can be taken to maintain the plant in a safe state or to bring it back into a safe state after anticipated operational occurrences and accident conditions.** | | The **AP1000** plant MCR (also see **AP1000** plant DCD [2] Section 3.1.1, GDC 19) provides the man-machine interfaces required to operate the plant safely and efficiently under normal conditions and to maintain it in a safe manner under accident conditions, including LOCAs (See **AP1000** plant DCD [2] Section 18.8). Simplified, passive, safety system designs are provided that do not rely upon operator action to maintain core cooling for DBAs. Operator actions are also not required to place the plant in a safe shutdown. | | |
|  |  | **Requirement 65: Control room (cont.)** | | The MCR/control support area HVAC subsystem of the nuclear island nonradioactive ventilation system allows access to and occupancy of the MCR under accident conditions. If ac power is unavailable for more than 10 minutes or if “high-high” particulate or iodine radioactivity is detected in the MCR supply air duct, which would lead to exceeding US NRC GDC 19 operator dose limits, the PMS automatically isolates the MCR and operator habitability requirements are then met by the main control room emergency habitability system. The main control room emergency habitability system is capable of providing emergency ventilation and pressurization for the MCR. The main control room emergency habitability system also provides emergency passive heat sinks for the MCR, I&C rooms, and dc equipment rooms. See **AP1000** plant DCD [2] Section 6.4.  In the event that the operators are forced to abandon the MCR, a remote shutdown workstation is provided with remote shutdown capability. A MCR evacuation is not assumed to occur simultaneously with DBEs. The remote shutdown workstation is described in the **AP1000** plant DCD [2] Section 7.4. | | |
| 6.39 | 1 | Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room against hazards such as high radiation levels resulting from accident conditions, release of radioactive material, fire, or explosive or toxic gases. | | Communication channels are available between the MCR and the Technical Support Center. Communications are also discussed in Reference 5, Section 3.  Also see response for Requirement 65. | | |
| 6.40 | 1 | Special attention shall be paid to identifying those events, both internal and external to the control room, that could challenge its continued operation, and the design shall provide for reasonably practicable measures to minimize the consequences of such events. | | The MCR is serviced by reliable and redundant non-safety and DiD power sources and heating, ventilation and air conditioning systems during normal operation.   * In the unlikely event that the normal power source or the HVAC system becomes unavailable, there are passive systems (batteries, compressed air) to support the MCR for up to 3 days. * The safety power sources and passive cooling system are designed to provide a habitable environment for the operating staff assuming that no ac power is available. Installed equipment provides for at least 3 days of operation, as stated above. After 3 days, it is possible to continue operation with the control room cooled and ventilated with circulation of outside air. * A mechanism is provided to allow the operating staff to transfer control from the MCR to the remote shutdown workstation. * The system prevents spurious signals caused by fire damage from being issued to components once transfer to the remote shutdown workstation has been affected.   Also refer to the **AP1000** plant DCD [2] Section 18.8 “Human System Interface Design” and the **AP1000** plant DCD [2] Section 7.4.3 “Safe Shutdown from Outside the Main Control Room”. | | |
| 6.40A | 1 | The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site. | | The **AP1000** plant design includes margin against the design basis natural hazards as discussed in [16] and in Appendix 12B of the **AP1000** plant PCSR [19]. | | |
|  |  | **Requirement 66: Supplementary control room**  **Instrumentation and control equipment shall be kept available, preferably at a single location (a supplementary control room) that is physically, electrically and functionally separate from the control room at the nuclear power plant. The supplementary control room shall be so equipped that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and essential plant variables can be monitored if there is a loss of ability to perform these essential safety functions in the control room.** | | The **AP1000** plant remote shutdown workstation is discussed in the **AP1000** plant DCD [2] Section 7.4.3. The Remote Shutdown Workstation is physically, electrically and functionally separated from the MCR. If temporary evacuation of the MCR is required because of some abnormal MCR condition, the operators can establish and maintain safe shutdown conditions for the plant from outside the MCR through the use of controls and monitoring located at the remote shutdown workstation. Safe shutdown is a stable plant condition that can be maintained for an extended period of time. In the event that access to the MCR is restricted, the plant is maintained in safe shutdown until the MCR can be re-entered. The remote shutdown workstation is designed to allow control of a shutdown following an evacuation of the control room, coincident with the loss of offsite power and a single active failure. No other DBE is postulated. | | |
| 6.41 | 1 | The requirements of para. 6.39 for taking appropriate measures and providing adequate information for the protection of occupants against hazards apply for the supplementary control room at the nuclear power plant. | | The remote shutdown workstation is designed to allow control of a shutdown following an evacuation of the control room, coincident with the loss of offsite power and a single active failure. No other DBE is postulated (i.e. it’s not postulated the use of the Remote Shutdown Workstation after a LOCA or after a severe accident). Communication is available in any case through the TSC. | | |
|  |  | **Requirement 67: Emergency control centre**  **The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards.** | | The **AP1000** plant DCD [2] Section 13.3 discusses Emergency Planning and Section 1.2.5 provides the locations of the technical support center, the operations support center and the decontamination facilities. The **AP1000** plant DCD [2] Section 9.4 provides a description of the HVAC systems for the MCR/control support area and the annex building. The **AP1000** plant DCD [2] Section 18.8 provides the high level requirements for the technical support center and the operations support center. The **AP1000** plant DCD [2] Section 7.5 identifies the plant variables that are provided for interface to the emergency planning areas. Communication interfaces among the MCR, the technical support center and the emergency planning centers are discussed in the **AP1000** plant DCD [2] Section 13.3.1. | | |
| 6.42 | 1 | Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided in the relevant emergency response facilities23. Each facility shall be provided with means of communication with, as appropriate, the control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.  *Footnote: 23 Emergency response facilities are addressed in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11]. For nuclear power plants, emergency response facilities (which are separate from the control room and the supplementary control room) include the technical support centre, the operational support centre and the emergency centre.* | | Information about important plant parameters and radiological conditions are made available in the MCR and TSC via the communication system (see **AP1000** plant DCD [2] Section 9.5.2). | | |
| 6.42 (cont.) | 1 |  | | The communications system provides effective interplant communications and effective plant-to-offsite communications during normal, maintenance, transient, fire, and accident conditions, including loss of offsite power. The communication system consists of the following subsystems:   * Wireless telephone system * Telephone/page system * Private automatic branch exchange system * Sound-powered system * Emergency offsite communications * Security communication system.   The communication system allows each guard, watchman, or armed response individual on duty to maintain continuous communication with an individual in each manned alarm station and with other agencies both onsite and offsite, as required by 10 CFR 73, Sections 55 (e) and (f). This is accomplished by both the private automatic branch exchange system and the wireless communication system. Each system can provide these communication functions.  Communication equipment used with respiratory protection devices will be designed and selected in accordance with EPRI NP-6559.  Also see response for Requirement 67. | | |
|  |  | **EMERGENCY POWER SUPPLY** | |  | | |
|  |  | **Requirement 68: Design for withstanding the loss of off-site power**  **The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions.** | | The IDS is the battery powered emergency power supply for safety functions after postulated initiating events. The system has sufficient capacity to achieve and maintain safe shutdown of the plant for 72 hours following a complete loss of all ac power sources without requiring load shedding for the first 24 hours. See **AP1000** plant DCD [2] Chapter 8.  Offsite power has no safety function due to the passive design of the **AP1000** plant. Therefore, redundant offsite power supplies are not required. The onsite standby power system powered by the two onsite standby diesel generators supplies power to selected loads in the event of loss of normal, and preferred ac power supplies. | | |
| 6.43 | 1 | The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity. | | See response for Requirement 68. | | |
| 6.44 | 1 | The combined means to provide emergency power (such as water, steam or gas turbines, diesel engines or batteries) shall have a reliability and type that are consistent with all the requirements of the safety systems to be supplied with power, and their functional capability shall be testable. | | IDS has sufficient capacity to achieve and maintain safe shutdown of the plant for 72 hours following a complete loss of all ac power sources without requiring load shedding for the first 24 hours. This system is designed with reliability consistent with all the requirements of the safety systems to be supplied with power. See **AP1000** plant DCD [2] Chapter 8. | | |
| 6.44A | 1 | The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply. | | As discussed in [14], [15], [16] and Appendix 12B of the AP1000 plant PCSR [19], core damage and spent fuel damage are prevented even if all power (onsite and offsite) is lost. | | |
| 6.44B | 1 | Equipment that is necessary to mitigate the consequences of melting of the reactor core shall be capable of being supplied by any of the available power sources. | | Core melt mitigation features can be supplied by any of the available power sources, except for the IDS which is dedicated to the safety systems. However this is considered acceptable:   * As discussed in [14], [15], [16] and Appendix 12B of the AP1000 plant PCSR [19], core damage and spent fuel damage are prevented even if all power (onsite and offsite) is lost. * Loss of offsite power event category does not significantly contribute to the AP1000 plant PRA (Chapter 19 of the **AP1000** plant DCD [2]). | | |
| 6.44C | 1 | The alternate power source shall be independent of and physically separated from the emergency power supply. The connection time of the alternate power source shall be consistent with the depletion time of the battery. | | As discussed in [14], [15], [16] and Appendix 12B of the AP1000 plant PCSR [19], core damage and spent fuel damage are prevented even if all power (onsite and offsite) is lost. | | |
| 6.44D | 1 | Continuity of power for the monitoring of the key plant parameters and for the completion of short term actions necessary for safety shall be maintained in the event of loss of the AC (alternating current) power sources. | | IDS has sufficient capacity to achieve and maintain safe shutdown of the plant for 72 hours following a complete loss of all ac power sources without requiring load shedding for the first 24 hours. | | |
| 6.45 | 1 | The design basis for any diesel engine or other prime mover24 that provides an emergency power supply to items important to safety shall include:  (a) The capability of the associated fuel oil storage and supply systems to satisfy the demand within the specified time period;  (b) The capability of the prime mover to start and to function successfully under all specified conditions and at the required time;  (c) Auxiliary systems of the prime mover, such as coolant systems.  *Footnote: 24 A prime mover is a component (such as a motor, solenoid operator or pneumatic operator) that converts energy into action when commanded by an actuation device.* | | The **AP1000** plant design does not use diesel generators to support the safety functions during accidents. The IDS does not require support systems to meet its safety function.  The onsite standby power system powered by the two onsite standby diesel generators supplies power to selected loads in the event of loss of normal and preferred ac power supplies. See **AP1000** plant DCD [2] Chapter 8. | | |
| 6.45A | 1 | The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.25  *Footnote: 25 Non-permanent equipment need not necessarily be stored on the site.* | | The **AP1000** plant design includes safety connections for non-permanent equipment. See [14]. | | |
|  |  | **SUPPORTING SYSTEMS AND AUXILIARY SYSTEMS** | |  | | |
|  |  | **Requirement 69: Performance of supporting systems and auxiliary systems.**  **The design of supporting systems and auxiliary systems shall be such as to ensure that the performance of these systems is consistent with the safety significance of the system or component that they serve at the nuclear power plant.** | | **AP1000** plant auxiliary systems are described in the **AP1000** plant DCD [2] Chapter 9. These systems are designed to perform reliably during normal plant operations. These systems are not required to perform safety functions during DBAs, other than the containment isolation function for those portions with a containment penetration. See **AP1000** plant DCD [2] Section 6.2.3 for description of the containment isolation function and Chapter 9 for a description of the auxiliary systems. | | |
|  |  | **Requirement 70: Heat transport systems**  **Auxiliary systems shall be provided as appropriate to remove heat from systems and components at the nuclear power plant that are required to function in operational states and in accident conditions.** | | The **AP1000** plant auxiliary systems that provide decay heat removal during normal operations include the normal residual heat removal system (**AP1000** plant DCD [2] Section 5.4.7), the spent fuel pool cooling system (**AP1000** plant DCD [2] Section 9.1.3), the component cooling water system (**AP1000** plant DCD [2] Section 9.2.2), and the service water system (**AP1000** plant DCD [2] Section 9.2.1).  Post accident heat removal is provided by the passive safety systems (**AP1000** plant DCD [2] Chapter 6 and Chapter 9, Section 9.1.3.4.3.). | | |
| 6.46 | 1 | The design of heat transport systems shall be such as to ensure that non-essential parts of the systems can be isolated. | | The design of the heat transport systems includes the capability to isolate non-essential parts. | | |
|  |  | **Requirement 71: Process sampling systems and post-accident sampling systems**  **Process sampling systems and post-accident sampling systems shall be provided for determining in a timely manner, the concentration of specified radionuclides in fluid process systems, and in gas and liquid samples taken from systems or from the environment, in all operational states and in accident conditions at the nuclear power plant.** | | The **AP1000** plant primary sampling system and secondary sampling system provide this capability and are described in the **AP1000** plant DCD [2] Sections 9.3.3 and 9.3.4.  In particular, the **AP1000** primary sampling system performs the following functions:   * Collects in normal operation mode both liquid and gaseous samples * Provides for local grab samples during normal operation mode   The PSS includes equipment to collect representative samples of the various process fluids, including RCS and containment air, in a manner that adheres to ALARA principles during both normal and post-accident conditions.  The PSS provides a way to monitor the plant and various system conditions using the collected and analyzed samples.  The results of the sample analyses are used to perform the following functions:   * Monitor core reactivity * Monitor fuel rod integrity | | |
|  |  | **Requirement 71: Process sampling systems and post-accident sampling systems (cont.)** | | * Evaluate ion exchanger (demineralizer) and filter performance * Specify chemical additions to the various systems; * Maintain acceptable hydrogen levels in the RCS * Detect radioactive material leakage   The PSS does not include seperate post-accident sampling capability. However, there are contingency plans for obtaining and analyzing highly radioactive samples of reactor coolant, containment sump, and containment atmosphere. These plans include the procedures to analyze, during the later stages of accident response, reactor coolant for boron, containment atmosphere for hydrogen and fission products, and containment sump water for pH.  The secondary sampling system delivers representative samples of fluids from secondary systems to sample analyzer packages. Continuous online secondary chemistry monitoring detects impurity ingress and provides early diagnosis of system chemistry excursions in the plant. Secondary sampling monitors send control signals to the turbine island chemical feed system that automatically injects corrosion control chemicals into the condensate and feedwater systems. | | |
|  |  | **Requirement 71: Process sampling systems and post-accident sampling systems (cont.)** | | Finally, the radiation monitoring system (RMS) (**AP1000** plant DCD [2] Section 11.5) provides plant effluent monitoring, process fluid monitoring, airborne monitoring, and continuous indication of the radiation environment in plant areas where such information is needed. Radiation monitors that have a safety function are qualified environmentally, seismically, or both. Class 1E radiation monitors conform to the separation criteria described in DCD Section 8.3.2 and to the fire protection criteria described in Section 9.5.1.  The RMS is installed permanently and operates in conjunction with regular and special radiation survey programs to assist in meeting applicable regulatory requirements. The RMS is divided functionally into two subsystems:   * Process, airborne, and effluent radiological monitoring and sampling * Area radiation monitoring | | |
| 6.47 | 1 | Appropriate means shall be provided at the nuclear power plant for the monitoring of activity in fluid systems that have the potential for significant contamination, and for the collection of process samples. | | See response for Requirement 71. In addition refer to the **AP1000** plant DCD [2] Section 9.3.5 “Equipment and Floor Drainage Systems”, Section 9.3.6. “Chemical & Volume Control System” and Chapter 11 “Radioactive Waste Management.” | | |
|  |  | **Requirement 72: Compressed air systems**  **The design basis for any compressed air system that serves an item important to safety at the nuclear power plant shall specify the quality, flow rate and cleanness of the air to be provided.** | | The **AP1000** plant compressed air system serves no safety function other than containment isolation. See the **AP1000** plant DCD [2] Section 9.3.1. | | |
|  |  | **Requirement 73: Air conditioning systems and ventilation systems**  **Systems for air conditioning, air heating, air cooling and ventilation shall be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain the required environmental conditions for systems and components important to safety in all plant states.** | | **AP1000** plant air-conditioning, heating, cooling, and ventilation systems are described in the **AP1000** plant DCD [2] Section 9.4. These systems are not required to perform safety functions during DBAs, other than the containment isolation function for those portions with a containment penetration. | | |
| 6.48 | 1-6 | Systems shall be provided for the ventilation of buildings at the nuclear power plant with appropriate capability for the cleaning of air:  (a) To prevent unacceptable dispersion of airborne radioactive substances within the plant;  (b) To reduce the concentration of airborne radioactive substances to levels compatible with the need for access by personnel to the area;  (c) To keep the levels of airborne radioactive substances in the plant below authorized limits and as low as reasonably achievable;  (d) To ventilate rooms containing inert gases or noxious gases without impairing the capability to control radioactive effluents;  (e) To control gaseous radioactive releases to the environment below the authorized limits on discharges and to keep them as low as reasonably achievable. | | The air-conditioning, heating, cooling, and ventilation system is comprised of the following systems that serve the various buildings and structures of the plant:   * Nuclear island nonradioactive ventilation system (**AP1000** plant DCD [2] Section 9.4.1) * Annex/auxiliary buildings nonradioactive HVAC system (**AP1000** plant DCD [2] Section 9.4.2) * Radiologically controlled area ventilation system (**AP1000** plant DCD [2] Section 9.4.3) * Containment recirculation cooling system (**AP1000** plant DCD [2] Section 9.4.6) * Containment air filtration system (**AP1000** plant DCD [2] Section 9.4.7) * Radwaste building HVAC system (**AP1000** plant DCD [2] Section 9.4.8) * Turbine building ventilation system (**AP1000** plant DCD [2] Section 9.4.9) * Diesel generator building heating and ventilation system (**AP1000** plant DCD [2] Section 9.4.10) * Health physics and hot machine shop HVAC system (**AP1000** plant DCD [2] Section 9.4.11)   **AP1000** plant air-conditioning, heating, cooling, and ventilation systems provide capabilities the required capabilities as described in the **AP1000** plant DCD [2] Section 9.4. The **AP1000** plant gaseous radwaste system provides control of gaseous releases as described in the **AP1000** plant DCD [2] Section 11.3. | | |
| 6.49 | 1 | Areas of higher contamination at the plant shall be maintained at a negative pressure differential (partial vacuum) with respect to areas of lower contamination and other accessible areas. | | This measure is applied in the **AP1000** plant systems described in the **AP1000** plant DCD [2] Section 9.4. | | |
|  |  | **Requirement 74: Fire protection systems**  **Fire protection systems, including fire detection systems and fire extinguishing systems, fire containment barriers and smoke control systems, shall be provided throughout the nuclear power plant, with due account taken of the results of the fire hazard analysis.** | | The **AP1000** plant fire protection system and measures are described in the **AP1000** plant DCD [2] Section 9.5.1.  To achieve the required high degree of fire safety, and to satisfy fire protection objectives, the **AP1000** plant is designed to:   * Prevent fire initiation by controlling, separating, and limiting the quantities of combustibles and sources of ignition. * Isolate combustible materials and limit the spread of fire by subdividing plant buildings into fire areas separated by fire barriers. * Separate redundant safe shutdown components and associated electrical divisions to preserve the capability to safely shut down the plant following a fire. * Provide the capability to safely shut down the plant using controls external to the MCR, should a fire require evacuation of the control room or damage the control room circuitry for safe shutdown systems. | | |
|  |  | **Requirement 74: Fire protection systems (cont.)** | | * Redundant trains of non-safety and DiD equipment used for normal plant operations (but not required for safe shutdown following a fire) are located in separate fire zones so that a fire within one train will not damage the redundant train. * Prevent smoke, hot gases, or fire suppressants from migrating from one fire area to another to the extent that they could adversely affect safe shutdown capabilities, including operator actions. * Provide confidence that failure or inadvertent operation of the fire protection system cannot prevent plant safety functions from being performed. * Preclude the loss of structural support, due to warping or distortion of building structural members caused by the heat from a fire, to the extent that such a failure could adversely affect safe shutdown capabilities. * Provide floor drains sized to remove expected firefighting water flow without flooding safety equipment. * Provide firefighting personnel access and life safety escape routes for each fire area. | | |
|  |  | **Requirement 74: Fire protection systems (cont.)** | | * Provide emergency lighting and communications to facilitate safe shutdown following a fire * Minimize exposure to personnel and releases to the environment of radioactivity or hazardous chemicals as a result of a fire   In addition, the fire protection system is designed to perform, among others, the following functions:   * Detect and locate fires and provide operator indication of the location (**AP1000** plant DCD [2] Section 9.5.1.2.1.2, Fire Detection and Alarm Systems) * Provide the capability to extinguish fires in any plant area, to protect site personnel, limit fire damage, and enhance safe shutdown capabilities * Supply fire suppression water at a flow rate and pressure sufficient to satisfy the demand of any automatic sprinkler system plus 500 gpm for fire hoses, for a minimum of 2 hours * Maintain 100 percent of fire pump design capacity, assuming failure of the largest fire pump or the loss of offsite power * • Following a safe shutdown earthquake, provide water to hose stations for manual firefighting in areas containing safe shutdown equipment | | |
| 6.50 | 1 | The fire protection systems installed at the nuclear power plant shall be capable of dealing safely with fire events of the various types that are postulated. | | The **AP1000** plant fire protection analysis in the **AP1000** plant DCD [2] Appendix 9A demonstrates the capability to deal with fire events. | | |
| 6.51 | 1 | Fire extinguishing systems shall be capable of automatic actuation where appropriate. Fire extinguishing systems shall be designed and located to ensure that their rupture or spurious or inadvertent operation would not significantly impair the capability of items important to safety. | | Automatic fire suppression systems are in accordance with Branch Technology Position (BTP) CMEB 9.5-1 and the applicable National Fire Protection Association (NFPA) standards, with consideration of the unique aspects of each application, including building characteristics, materials of construction, environmental conditions, fire area contents, and adjacent structures.  Fixed automatic fire suppression systems are provided based on the results of the fire protection analysis. Fire extinguishing systems are designed and located to ensure that their rupture or spurious or inadvertent operation does not significantly impair the capability of items important to safety.  See **AP1000** plant DCD [2] Section 9.5.1. | | |
| 6.52 | 1 | Fire detection systems shall be designed to provide operating personnel promptly with information on the location and spread of any fires that start. | | Fire detection and alarm systems are provided where required by the fire protection analysis, in accordance with BTP CMEB 9.5-1 and NFPA 72. Fire detection and alarm systems are generally in accordance with NFPA 804.  See **AP1000** plant DCD [2] Section 9.5.1. | | |
| 6.53 | 1 | Fire detection systems and fire extinguishing systems that are necessary to protect against a possible fire following a postulated initiating event shall be appropriately qualified to resist the effects of the postulated initiating event. | | The **AP1000** plant fire protection analysis in the **AP1000** plant DCD [2] Appendix 9A demonstrates the capability to deal with fire events. | | |
| 6.54 | 1 | Non-combustible or fire retardant and heat resistant materials shall be used wherever practicable throughout the plant, in particular in locations such as the containment and the control room. | | Fire prevention and control features are identified in the **AP1000** plant DCD [2] Section 9.5.1.2.1.1. | | |
|  |  | **Requirement 75: Lighting systems**  **Adequate lighting shall be provided in all operational areas of the nuclear power plant in operational states and in accident conditions.** | | The **AP1000** plant lighting system is described in the **AP1000** plant DCD [2] Section 9.5.3. The plant lighting system includes normal, emergency, panel, and security lighting. The normal lighting provides normal illumination during plant operating, maintenance, and test conditions. The emergency lighting provides illumination in areas where emergency operations are performed upon loss of normal lighting. The panel lighting in the control room is designed to provide the minimum illumination required at the safety panels. The security lighting system is described in separate security documents referred to in the **AP1000** plant DCD [2] Section 13.6. | | |
|  |  | **Requirement 76: Overhead lifting equipment**  **Overhead lifting equipment shall be provided for lifting and lowering items important to safety at the nuclear power plant, and for lifting and lowering other items in the proximity of items important to safety.** | | **AP1000** plant overhead heavy load handling systems are described in the **AP1000** plant DCD [2] Section 9.1.5. The polar crane, cask handling crane, containment equipment hatch hoist, and containment maintenance hatch hoist are single-failure-proof systems and are classified as seismic Category I. They are designed to support a critical load during and after a safe shutdown earthquake. The equipment and maintenance hatches are required to be operational after a safe shutdown earthquake. | | |
| 6.55 | 1 | The overhead lifting equipment shall be designed so that:   1. Measures are taken to prevent the lifting of excessive loads; 2. Conservative design measures are applied to event any unintentional dropping of loads that could affect items important to safety; 3. The plant layout permits the safe movement of the overhead lifting equipment and of items being transported; 4. Such equipment can be used only in specified plant states (by means of safety interlocks on the crane); 5. Such equipment for use in areas where items important to safety are located is seismically qualified. | | See response for Requirement 76.  (a) Lifting devices are installed in the plant to prevent the lifting of excessive loads during maintenance operations.  (b) Measures and procedures are in place to avoid that unintentional dropping of loads that could affect items important to safety  (c) The plant layout account for the safe movement of the overhead lifting equipment and transported items  (d) Standard engineering practice. See **AP1000** plant DCD [2] Section 9.5.1.  (e) According to Seismic Classification criteria all the equipment and structures whose failure following a seismic event may impact SSC important to safety must be seismically qualified (as minimum SC2). | | |
|  |  | **OTHER POWER CONVERSION SYSTEMS** | |  | | |
|  |  | **Requirement 77: Steam supply system, feedwater system and turbine generators**  **The design of the steam supply system, feedwater system and turbine generators for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in operational states or accident conditions.** | | The **AP1000** plant steam and power conversion systems are described in the **AP1000** plant DCD [2] Chapter 10. Spring-loaded safety valves are provided on both main steam lines, in accordance with the ASME Code, Section III. The pressure relief capacity of the safety valves is such that the energy generated at the high-flux reactor trip setting can be dissipated through this system without overpressurizing the reactor coolant pressure boundary.  In addition, the shell sides of the feedwater heaters and the moisture separator/reheaters are provided with overpressure protection in accordance with ASME Boiler and Pressure Vessel Code, Section VIII, Division 1, or equivalent standards. | | |
| 6.56 | 1 | The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and accident conditions. | | The main steam supply system is provided with a main steam isolation valve and associated bypass valve on each main steam line from its respective steam generator. These valves isolate the secondary side of each of the steam generators to prevent the uncontrolled blowdown of more than one steam generator. The main steam system also includes appropriate valves to isolate the non-safety portions of the system. See **AP1000** plant DCD [2] Section 10.3. | | |
| 6.57 | 1 | The steam supply system and feedwater systems shall be of sufficient capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions. | | These systems are designed to address AOOs. For example, in the event of turbine trip, steam is bypassed to the condenser via the turbine bypass valves and, if required, to the atmosphere via the atmospheric relief valves. Steam relief permits energy removal from the RCS. Load rejection capability is discussed in the **AP1000** plant DCD [2] Sections 10.3.2.3.1 and 15.2.2. | | |
| 6.58 | 1 | The turbine generators shall be provided with appropriate protection such as overspeed protection and vibration protection, and measures shall be taken to minimize the possible effects of turbine generated missiles on items important to safety. | | The overspeed trips for the **AP1000** plant turbine consist of a 110% trip in the emergency trip system and a 111% backup trip in the OA controller. The overspeed protection system will function for all abnormal conditions, including a single failure of any component or subsystem. Vibration at turbine bearings is monitored and alarmed (see **AP1000** plant DCD [2] Section 10.2.2.5). The turbine generator is located north of the nuclear island with its shaft oriented north-south. In this orientation, the potential for damage from turbine missiles is negligible. Safety SSCs are located outside the high‑velocity, low-trajectory missile strike zone, as defined by Regulatory Guide 1.115. Thus, postulated low-trajectory missiles cannot directly strike safety areas (see **AP1000** plant DCD [2] Section 3.5.1.3). | | |
|  |  | **TREATMENT OF RADIOACTIVE EFFLUENTS AND RADIOACTIVE WASTE** | |  | | |
|  |  | **Requirement 78: Systems for treatment and control of waste**  **Systems shall be provided for treating solid radioactive waste and liquid radioactive waste at the nuclear power plant to keep the amounts and concentrations of radioactive releases below the authorized limits on discharges and as low as reasonably achievable.** | | The **AP1000** plant is designed with administrative programs and procedures to maximize the incorporation of good engineering practices and lessons learned to accomplish ALARA objectives.  The ALARA policy is applied during the design of **AP1000** plant. The design is reviewed for ALARA considerations and updated and modified as experience from operating plants is applied. ALARA reviews include the plant design and integrated layout, considering shielding, ventilation, and monitoring instrument designs as they relate to traffic control, security, access control and health physics.  Radwaste systems for the **AP1000** plant are discussed in the **AP1000** plant DCD [2] Chapter 11. Radiation Protection is dealt with in the **AP1000** plant DCD [2] Chapter 12.  The **AP1000** plant is provided with systems that are able to treat liquid, gas & solid radioactive wastes. In particular:  The liquid waste management systems include the systems that may be used to process and dispose of liquids containing radioactive material. These include the following: | | |
|  |  |  | | * Steam generator blowdown processing system (**AP1000** plant DCD [2] Section 10.4.8); * Radioactive waste drain system (**AP1000** plant DCD [2] Section 9.3.5); * Liquid radwaste system (**AP1000** plant DCD [2] Section 11.2).   Gaseous Wastes:  The **AP1000** plant gaseous radwaste system is designed to perform the following major functions:   * Collect gaseous wastes that are radioactive or hydrogen bearing * Process and discharge the waste gas, keeping off-site releases of radioactivity within acceptable limits.   Solid Radwaste  The solid waste management system is designed to collect and accumulate spent ion exchange resins and deep bed filtration media, spent filter cartridges, dry active wastes, and mixed wastes generated as a result of normal plant operation, including AOOs.  This system does not handle large, radioactive waste materials such as core components or radioactive process wastes from the plant's secondary cycle. | | |
| 6.59 | 1 | Systems and facilities shall be provided for the management and storage of radioactive waste on the nuclear power plant site for a period of time consistent with the availability of the relevant disposal option. | | These requirements are met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Chapter 11 and the solid waste management system is presented in the **AP1000** plant DCD [2] Section 11.4.  In particular refer to the **AP1000** plant DCD [2] Section 11.4.2.3.3 “Dry Waste Processing Operations” and the **AP1000** plant DCD [2] Section 11.4.2.4 “Waste Processing and Disposal Alternatives.” | | |
| 6.60 | 1 | The design of the plant shall incorporate appropriate features to facilitate the movement, transport and handling of radioactive waste. Consideration shall be given to the provision of access to facilities and to capabilities for lifting and for packaging. | | These requirements are met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Chapter 11.  In particular the **AP1000** plant DCD [2] Section 11.4.1.3 specifies that “Provisions are made in the auxiliary and radwaste buildings to use mobile radwaste processing systems for processing and packaging each waste stream including concentration and solidification of chemical wastes from the liquid waste management system, spent resin dewatering, spent filter cartridge encapsulation and dry active waste sorting and compaction.” | | |
|  |  | **Requirement 79: Systems for treatment and control of effluents**  **Systems shall be provided at the nuclear power plant for treating liquid and gaseous radioactive effluents to keep their amounts below the authorized limits on discharges and as low as reasonably achievable.** | | These requirements are met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Chapter 11.  Also refer to the **AP1000** plant DCD [2] Section 12.1 which discuss the ALARA principles and application to the **AP1000** plant design and response for Requirement 78.  In addition, during the UK GDA process, an integrated waste management strategy was developed to ensure that radioactive material and radwastes generated by the **AP1000** plant are managed in a manner which minimizes the need for future processing, and that is compatible with anticipated facilities for ultimate disposal or end-use [6]. | | |
| 6.61 | 1 | Liquid and gaseous radioactive effluents shall be treated at the plant so that exposure of members of the public due to discharges to the environment is as low as reasonably achievable. | | These requirements are met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Sections 11.2 and 11.3.  Please also refer to the **AP1000** plant DCD [2] Section 12.1 that discusses the ALARA principles and application to the **AP1000** plant and response to Requirements 78 and 79. | | |
| 6.62 | 1 | The design of the plant shall incorporate suitable means to keep radioactive liquids releases to the environment as low as reasonably achievable and to ensure that radioactive releases remain below the authorized limits on discharges. | | These requirements are met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Section 11.2.3.  Please also refer to the **AP1000** plant DCD [2] Section 12.1 that discusses the ALARA principles and application to the **AP1000** plant and response to Requirements 78 and 79 | | |
| 6.63 | 1 | The cleanup equipment for the gaseous radioactive substances shall provide the necessary retention factor to keep radioactive releases below the authorized limits on discharges. Filter systems shall be designed so that their efficiency can be tested, their performance and function can be regularly monitored over their service life, and filter cartridges can be replaced while maintaining the throughput of air. | | These requirements are met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Section 11.3.3.  The gaseous radwaste system is designed to reduce the controlled activity releases in support of the overall **AP1000** plant release goals. The proper performance of the gaseous radwaste system depends upon delay of gaseous radionuclides by chemical adsorption on activated carbon. As the radionuclides are delayed, they decay and are no longer available for release to the environment. The rate of release and site boundary dose rates have been evaluated based upon the quantity of activated carbon in a delay bed being at least 80 cubic feet.  Two activated carbon delay beds in series are provided. Together, the beds provide 100 percent of the stated system capacity under design basis conditions. During normal operation a single bed provides adequate performance. This provides operational flexibility to permit continued operation of the gaseous radwaste system in the event of operational upsets in the system that requires isolation of one bed. | | |
|  |  | **FUEL HANDLING AND STORAGE SYSTEMS** | |  | | |
|  |  | **Requirement 80: Fuel handling and storage systems**  **Fuel handling and storage systems shall be provided at the nuclear power plant to ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.** | | **AP1000** plant fuel handling and storage systems are described in the **AP1000** plant DCD [2] Section 9.1. These systemsensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.  The New Fuel Storage is discussed in the **AP1000** plant DCD [2] Section 9.1.1.  Spent Fuel Storage is discussed in the **AP1000** plant DCD [2] Section 9.1.2.  The **AP1000** plant DCD [2] Section 9.1.4 discusses the Light Load Handling System (Related to Refueling).  Safety evaluations for the above are reported in the **AP1000** plant DCD [2] Sections 9.1.1.3, 9.1.2.3 and 9.1.4.3. | | |
| 6.64 | 1 | The design of the plant shall incorporate appropriate features to facilitate the lifting, movement and handling of fresh fuel and spent fuel. | | The **AP1000** plant fuel handling systems are described in the **AP1000** plant DCD [2] Section 9.1.4.  The light load handling system (**AP1000** plant DCD [2] Section 9.1.4) consists of the equipment and structures needed for the refueling operation. This equipment is comprised of fuel assemblies, core component and reactor component hoisting equipment, handling equipment, and a fuel transfer system. The structures associated with the fuel handling equipment are the refueling cavity, the transfer canal, the fuel transfer tube, the spent fuel pool, the cask loading area, the new fuel storage area, and the new fuel receiving and inspection area. | | |
| 6.65 | 1 | The design of the plant shall be such as to prevent any significant damage to items important to safety during the transfer of fuel or casks, or in the event of fuel or casks being dropped. | | The **AP1000** plant handling systems meet this requirement as discussed in the **AP1000** plant DCD [2] Sections 9.1.4 and 9.1.5. | | |
| 6.66 | 1 | The fuel handling and storage systems for irradiated and non-irradiated fuel shall be designed:  (a) To prevent criticality by a specified margin, by physical means or by means of physical processes, and preferably by the use of geometrically safe configurations, even under conditions of optimum moderation;  (b) To permit inspection of the fuel;  (c) To permit maintenance, periodic inspection and testing of components important to safety;  (d) To prevent damage to the fuel;  (e) To prevent the dropping of fuel in transit;  (f) To provide for the identification of individual fuel assemblies;  (g) To provide proper means for meeting the relevant requirements for radiation protection;  (h) To ensure that adequate operating procedures and a system of accounting for, and control of, nuclear fuel can be implemented to prevent any loss of, or loss of control over, nuclear fuel. | | These requirements are met for the **AP1000** plant. New fuel storage is discussed in the **AP1000** plant DCD [2] Section 9.1.1. The Spent Fuel Storage and Spent Fuel Pool Cooling System is discussed in the **AP1000** plant DCD [2] Section 9.1.2. The Spent Fuel Cask Loading and Shipping (health physics facility design) is discussed in the **AP1000** plant DCD [2] Section 12.5.3.4. The fuel handling dose assessment is discussed in the **AP1000** plant DCD [2] Section 12.4.1.6.  **New Fuel Rack**  The new fuel rack, being a seismic Category I structure, is designed to withstand normal and postulated dead loads, live loads, loads resulting from thermal effects, and loads caused by the safe shutdown earthquake event.  The design of the new fuel rack is such that Keff (with all biases and uncertainties) remains less than or equal to 0.95 with new fuel of the maximum design basis enrichment. For a postulated accident condition of flooding of the new fuel storage pit with unborated water, Keff does not exceed 0.98.  The criticality evaluation considers the inherent neutron absorbing effect of the materials of construction, including fixed neutron absorbing "poison" material. | | |
| 6.66 (cont.) | 1 |  | | **Spent Fuel Pool**  Spent fuel is stored in high density racks which include integral neutron absorbing material to maintain the required degree of subcriticality. The racks are designed to store fuel of the maximum design basis enrichment. Each rack in the spent fuel pool consists of an array of cells interconnected to each other at several elevations and to a thick base plate at the bottom elevation. These rack modules are free-standing, neither anchored to the pool floor nor braced to the pool wall. The spent fuel storage racks include storage locations for 884 fuel assemblies and five defective fuel assemblies. | | |
| 6.67 | 1 | In addition, the fuel handling and storage systems for irradiated fuel shall be designed:  (a) To permit adequate removal of heat from the fuel in operational states and in accident conditions;  (b) To prevent the dropping of spent fuel in transit;  (c) To prevent causing unacceptable handling stresses on fuel elements or fuel assemblies;  (d) To prevent the potentially damaging dropping on the fuel of heavy objects such as spent fuel casks, cranes or other objects;  (e) To permit safe keeping of suspect or damaged fuel elements or fuel assemblies;  (f) To control levels of soluble absorber if this is used for criticality safety;  (g) To facilitate maintenance and future decommissioning of fuel handling and storage facilities;  (h) To facilitate decontamination of fuel handling and storage areas and equipment when necessary;  (i) To accommodate, with adequate margins, all the fuel removed from the reactor in accordance with the strategy for core management that is foreseen and the amount of fuel in the full reactor core;  (j) To facilitate the removal of fuel from storage and its preparation for off-site transport. | | These requirements are met for the **AP1000** plant.  The Spent Fuel Storage and Spent Fuel Pool Cooling System is discussed in the **AP1000** plant DCD [2] Section 9.1.2. Sizing criteria for heat transfer are illustrated in the **AP1000** plant DCD [2] Section 9.1.3.1.3. Abnormal and accidental conditions are addressed in Section 9.1.3.4.3.  In the unlikely event of dropping a fuel assembly, accidental deformation of the rack is determined and evaluated in the criticality analysis to demonstrate that it does not cause the criticality criterion to be violated. The analysis considers only the case of a dropped spent, irradiated fuel assembly in a flooded pool and takes credit for dissolved boron in the water.  The Spent Fuel Cask Loading and Shipping (health physics facility design) is discussed in the **AP1000** plant DCD [2] Section 12.5.3.4.  The fuel handling dose assessment is discussed in the **AP1000** plant DCD [2] Section 12.4.1.6. | | |
| 6.68 | 1-2 | For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is ‘practically eliminated’26 and so as to avoid high radiation fields on the site. The design of the plant:  (a) Shall provide the necessary fuel cooling capabilities;  (b) Shall provide features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break;  (c) Shall provide a capability to restore the water inventory.  The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of spent fuel and for providing shielding against radiation.27  *Footnote: 26 The possibility of certain conditions arising may be considered to have been ‘practically eliminated’ if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise.*  *27 Non-permanent equipment need not necessarily be stored on the site.* | | These requirements are met for the **AP1000** plant. The Spent Fuel Storage and Spent Fuel Pool Cooling System is discussed in the **AP1000** plant DCD [2] Chapter 9.1.3.  The spent fuel pool cooling system is designed to remove decay heat which is generated by stored fuel assemblies from the water in the spent fuel pool. This is done by pumping the high temperature water from within the fuel pool through a heat exchanger, and then returning the water to the pool. A secondary function of the spent fuel pool cooling system is clarification and purification of the water in the spent fuel pool, the transfer canal, and the refueling water. A listing of the major functions of the spent fuel pool cooling system and the corresponding modes of operation is provided below:   * **Spent fuel pool cooling** - Remove heat from the water in the spent fuel pool during operation to maintain the pool water temperature within acceptable limits. * **Spent fuel pool purification** - Provide purification and clarification of the spent fuel pool water during operation. * **Refueling cavity purification** - Provide purification of the refueling cavity during refueling operations. | | |
| 6.68 (cont.) | 1 |  | | * **Water transfers** - Transfer water between the in‑containment refueling water storage tank and the refueling cavity during refueling operations. * **In-containment refueling water storage tank purification** - Provide purification and cooling of the in-containment refueling water storage tank during normal operation.   Finally, the Spent Fuel Pool is designed such that, even following a safe shutdown earthquake, the spent fuel remains covered with water [15]. | | |
| 6.68A | 1 | 6.68A. The design shall include the following:  (a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool;  (b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool;  (c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool;  (d) Means for monitoring and controlling the water chemistry for operational states. | | (a) During normal operation and AOOs (when ac power is available and hence when the active DiD system should be available to cool the spent fuel pool), the spent fuel pool temperature is monitored.  (b) For all DBAs and for DEC (as long as power – from the safety IDS or another source - is available), the spent fuel pool level is monitored.  (c) & (d) Sampling of the SFP water for chemistry (boron, conductivity, pH, impurities, corrosion product metals, etc.) and activity (gross activity, corrosion product activity, fission product activity, I-131, tritium, etc.) is conducted periodically. Grab samples can be taken in the individual spent fuel pool cooling system lines. | | |
|  |  | **RADIATION PROTECTION** | |  | | |
|  |  | **Requirement 81: Design for radiation protection**  **Provision shall be made for ensuring that doses to operating personnel at the nuclear power plant will be maintained below the dose limits and will be kept as low as reasonably achievable, and that the relevant dose constraints will be taken into consideration.** | | This requirement is met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] Sections 12.1 and 12.3. The design is reviewed for ALARA considerations and updated and modified as experience from operating plants is applied. ALARA reviews include the plant design and integrated layout, considering shielding, ventilation, and monitoring instrument designs as they relate to traffic control, security, access control and health physics. | | |
| 6.69 | 1 | Radiation sources throughout the plant shall be comprehensively identified and exposures and radiation risks associated with them shall be kept as low as reasonably achievable28, the integrity of the fuel cladding shall be maintained, and the generation and transport of corrosion products and activation products shall be controlled.  *Footnote: 28 Requirements on radiation protection and the safety of radiation sources for facilities and activities are established in GSR Part 3 [9].* | | The **AP1000** plant DCD [2] Section 12.2 describes the sources of radiation that form the basis for shielding design calculations and the sources of airborne radioactivity used for the design of personnel protection measures and dose assessment for ALARA purposes.  The following radiation sources are comprehensively identified for each system and operational mode. A complete discussion can be found in the **AP1000** plant DCD [2] Section 12.1:  **AP1000** plant DCD [2] Section 12.2.1 Contained Sources  Sources for Full-Power Operation  Sources for Shutdown  Sources for the Core Melt Accident  **AP1000** plant DCD [2] Section 12.2.2 Airborne Radioactive Material Sources  Containment Atmosphere  Fuel-Handling Area Atmosphere  Auxiliary Building Atmosphere  In particular, sources of radiation in the RCS during the power operation are fission products released from fuel and activation of the coolant and of corrosion products that are circulated in the reactor coolant. These sources and their bases are described in the **AP1000** plant DCD [2] Section 11.1. | | |
| 6.69 (cont.) | 1 |  | | The activation product, nitrogen-16 (N-16), is the predominant contributor to the activity in the reactor coolant pumps, steam generators, and reactor coolant piping during operation. **AP1000** plant DCD [2] Table 12.2-3 presents the reactor coolant N-16 activity as a function of transport time in a reactor coolant loop. The N-16 activity for the pressurizer is tabulated in the **AP1000** plant DCD [2] Table 12.2-4.  Fission and corrosion product activities circulating in the RCS and out-of-core crud deposits comprise the remaining significant radiation sources during full-power operation. The fission and corrosion product activities circulating in the reactor coolant are given in the **AP1000** plant DCD [2] Section 11.1. The fission and corrosion product source strengths and specific activities in the pressurizer liquid and vapor phases are given in the **AP1000** plant DCD [2] Table 12.2-5.  The isotopic composition and specific activity of typical out-of-core crud deposits are given in the **AP1000** plant DCD [2] Table 12.2‑6. Typically, one milligram of deposited crud material is found on one square centimeter of a relatively smooth surface. This may be as much as 50 times higher in crud trap areas. Crud trap areas are generally locations of high turbulence, areas of high momentum change, gravitational sedimentation areas, high affinity material areas, and possibly thin boundary layer regions. | | |
| 6.70 | 1 | Materials used in the manufacture of structures, systems and components shall be selected to minimize activation of the material as far as reasonably practicable. | | These requirements are met for the **AP1000** plant. The **AP1000** plant DCD [2] Section 12.3 identifies the specific **AP1000** plant design features for maintaining personnel exposure ALARA. These include, not only material selection but also design of components and systems, selection of reliable components, layout arrangement, automatic & remote controls and handling and in general minimization and optimization of the time required to perform maintenance operation in radiation fields.  Equipment specifications for components exposed to high temperature reactor coolant contain limitations on the cobalt content of the base metal as given in the **AP1000** plant DCD [2] Table 12.3-1. The use of hard facing material with cobalt content such as stellite is limited to applications where its use is necessary for reliability considerations. Nickel-based alloys in the RCS (Co‑58 is produced from activation of Ni-58) are similarly used only where component reliability may be compromised by the use of other materials. The major use of nickel-based alloys in the RCS is the Inconel® steam generator tubes.  General prohibitions on antimony and other low melting point metals are contained in the **AP1000** plant DCD [2] Section 6.1.1. In addition, the reactor coolant pump mechanical design criteria prohibit antimony completely from the reactor coolant pump and its bearings. | | |
| 6.71 | 1 | For the purposes of radiation protection, provision shall be made for preventing the release or the dispersion of radioactive substances, radioactive waste and contamination at the plant. | | The **AP1000** plant design meets this requirement. The **AP1000** plant DCD [2] Section 12.3 identifies the specific **AP1000** plant design features for maintaining personnel exposure ALARA.  The **AP1000** plant DCD [2] Chapter 11 identifies the radioactive waste management systems that are designed to control, collect, process, handle, store, and dispose of liquid radioactive waste generated as the result of normal operation, including AOOs.  In addition the **AP1000** plant ER [6] has been prepared to consolidate and summarize the environmental information in the **AP1000** plant DCD [2] and to supplement the environmental information to meet the environmental requirements of the UK GDA process.  Finally, [7] addresses the release and dispersion of radioactive substances derived from operation in the long term (Geological Disposal). | | |
| 6.72 | 1 | The plant layout shall be such as to ensure that access of operating personnel to areas with radiation hazards and areas of possible contamination is adequately controlled, and that exposures and contamination are prevented or reduced by this means and by means of ventilation systems. | | The **AP1000** plant design meets this requirement. The **AP1000** plant DCD [2] Section 12.3 identifies the specific **AP1000** plant design features for maintaining personnel exposure ALARA.  Radiation Zoning and Access Control is discusses in the **AP1000** plant DCD [2] Section 12.3.1.2. | | |
| 6.72 (cont.) | 1 |  | | Access to areas inside the plant structures and plant yard area is regulated and controlled by posting of radiation signs, control of personnel, and use of alarms and locks (**AP1000** plant DCD [2] Section 12.5). During plant operation, access to radiologically restricted areas is through the access control area in the annex building.  plant areas are categorized into radiation zones according to design basis radiation levels and anticipated personnel occupancy with consideration given toward maintaining personnel exposures ALARA and within the standards of 10 CFR 20. Rooms, corridors, and pipeways are evaluated for potential radiation sources during normal, shutdown, spent resin transfer, and emergency operations; for maintenance occupancy requirements; for general access requirements; and for material exposure limits to determine appropriate zoning. Each radiation zone defines the radiation level range expected in the zone.  Based on actual operating plant data, ingress or egress of plant operating personnel to radiologically restricted areas is controlled and monitored as discussed in the **AP1000** plant DCD [2] Section 12.3.5 such that radiation levels and exposures are within the limits prescribed in 10 CFR 20. | | |
| 6.73 | 1 | The plant shall be divided into zones that are related to their expected occupancy, and to radiation levels and contamination levels in operational states (including refuelling, maintenance and inspection) and to potential radiation levels and contamination levels in accident conditions. Shielding shall be provided so that radiation exposure is prevented or reduced. | | The **AP1000** plant design meets this requirement. The **AP1000** plant DCD [2] Section 12.3 identifies the specific **AP1000** plant zoning and shielding considerations.  Also see response for Paragraph 6.72. | | |
| 6.74 | 1 | The plant layout shall be such that the doses received by operating personnel during normal operation, refuelling, maintenance and inspection can be kept as low as reasonably achievable, and due account shall be taken of the necessity for any special equipment to be provided to meet these requirements. | | The **AP1000** plant design meets this requirement. The **AP1000** plant DCD [2] Section 12.4 provides the **AP1000** plant personnel dose assessments.  Also see response for Paragraph 6.72. | | |
| 6.75 | 1 | Plant equipment subject to frequent maintenance or manual operation shall be located in areas of low dose rate to reduce the exposure of workers. | | The **AP1000** plant design meets this requirement. The **AP1000** plant DCD [2] Section 12.3 identifies the specific **AP1000** plant design features for maintaining personnel exposure ALARA.  Systems containing radioactivity and other sources of radiation are identified for four plant conditions defined in the **AP1000** plant DCD [2] Section 12.3.2.1. Shielding is provided to attenuate direct radiation through walls and penetrations and scattered radiation to less than the upper limit of the radiation zone for each area shown in the **AP1000** plant DCD [2] Figure 12.3-1. Design criteria for shield penetrations are consistent with the recommendations of Regulatory Guide 8.8 and are described in the **AP1000** plant DCD [2] Section 12.3.1.1.2. | | |
| 6.75 (cont.) | 1 |  | | In those systems where process equipment is a major radiation source; pumps, valves, and instruments are separated from the process component. This allows servicing and maintenance of these items in reduced radiation zones. Control panels are located in low radiation zones.  Major components such as tanks, demineralizers, and filters in radioactive systems are located in shielded compartments insofar as practical. Labyrinth shields or shielding doors are provided for compartments where radiation could stream or scatter to access areas and exceed the radiation zone dose limits for those areas. For potentially high radiation components (such as ion exchangers, filters and spent resin tanks), shielded compartments with hatch openings or removable shield walls are used. Equipment in nonradioactive systems that requires lubrication is located in low radiation zones. Wherever practicable, lubrication of equipment in high radiation areas is achieved with the use of tube-type extensions to reduce exposure during maintenance. | | |
| 6.75 (cont.) | 1 |  | | Exposure from routine in-plant inspection is controlled by locating, whenever practicable, inspection points in low-background radiation areas. Radioactive and nonradioactive systems are separated as far as practicable to limit radiation exposure from routine inspection of nonradioactive systems. For radioactive systems, emphasis is placed on adequate space and ease of motion in a properly shielded inspection area. Where longer times for routine inspection are required and permanent shielding is not feasible, space for portable shielding is provided.  Materials used in shielding typically include lead, steel, water, and concrete. The material used for most of the plant shielding is ordinary concrete with a bulk density of approximately 140 lb/ft3. Whenever poured-in-place concrete has been replaced by concrete blocks, an equivalent shielding basis as determined by the density of the concrete block is selected. Steel is used as shielding in the CVS and other modules, as well as around the reactor vessel flange at the floor of the refueling cavity. Water is used as the primary shield material for areas above the spent fuel storage area and refueling cavity during refueling operations. | | |
| 6.76 | 1 | Facilities shall be provided for decontamination of operating personnel and plant equipment. | | The health physics area contains the personnel contamination monitoring equipment, decontamination shower facilities, and first-aid equipment (**AP1000** plant DCD [2] Section 12.5.2.2). The **AP1000** plant annex building includes a hot machine shop for servicing radiological control area equipment. The hot machine shop includes decontamination facilities including a portable decontamination system that may be used for decontamination operations throughout the nuclear island (**AP1000** plant DCD [2] Section 1.2.5). | | |
|  |  | **Requirement 82: Means of radiation monitoring**  **Equipment shall be provided at the nuclear power plant to ensure that there is adequate radiation monitoring in operational states and design basis accident conditions and, as far as is practicable, in design extension conditions.** | | The **AP1000** plant design meets this requirement. The **AP1000** plant RMS (**AP1000** plant DCD [2] Section 11.5) provides plant effluent monitoring, process fluid monitoring, airborne monitoring, and continuous indication of the radiation environment in plant areas where such information is needed. Radiation monitors that have a safety function are qualified environmentally, seismically, or both. | | |
|  |  | **Requirement 82: Means of radiation monitoring (cont.)** | | Class 1E radiation monitors conform to the separation criteria described in the **AP1000** plant DCD [2] Section 8.3.2 and to the fire protection criteria described in the **AP1000** plant DCD [2] Section 9.5.1. Equipment qualification requirements, including seismic qualification requirements and general location information for radiation monitors are listed in the **AP1000** plant DCD [2] Section 3.11. Seismic Categories for the buildings housing radiation monitors are listed in the **AP1000** plant DCD [2] Section 3.2.  The RMS is installed permanently and operates in conjunction with regular and special radiation survey programs to assist in meeting applicable regulatory requirements. The RMS is designed in accordance with ANSI N13.1-1969. The process monitors are designed in accordance with ANSI-N42.18-1980.  The RMS is divided functionally into two subsystems:   * Process, airborne, and effluent radiological monitoring and sampling * Area radiation monitoring | | |
|  |  | **Requirement 82: Means of radiation monitoring (cont.)** | | **Safety Design Basis**  While the RMS is primarily a surveillance system, certain detector channels perform safety functions. The components used in these channels meet the qualification requirements for safety equipment as described in the **AP1000** plant DCD [2] Section 7.1.4.  Channel and equipment redundancy is provided for safety monitors to maintain the safety function in case of a single failure.  The design objectives of the RMS during postulated accidents are:   * Initiate containment air filtration isolation in the event of abnormally high radiation inside the containment (High-1) * Initiate normal residual heat removal system suction line containment isolation in the event of abnormally high radiation inside the containment (High-2) * Initiate MCR supplemental filtration in the event of abnormally high gaseous radioactivity in the MCR supply air * Initiate MCR ventilation isolation and actuate the main control room emergency habitability system in the event of abnormally high particulate or iodine radioactivity in the MCR supply air | | |
|  |  | **Requirement 82: Means of radiation monitoring (cont.)** | | * Provide long-term post-accident monitoring (using both safety and non-safety monitors)   The scope of the RMS for post-accident monitoring is set forth in US NRC GDC 64 and in the provisions of Regulatory Guide 1.97.  **Power Operation Design Basis**  The RMS is designed to support the requirements of 10 CFR 20 and to provide:   * Equipment to meet the applicable regulatory requirements for both normal operation and transient events * Data to aid plant health physics personnel in limiting release of radioactivity to the environment and limiting exposure of operation and maintenance personnel to meet ALARA guidance * Early indication of a system or equipment malfunction that could result in excessive radiation dose to plant personnel or lead to plant damage * Data collection and data storage to support compliance reporting for the applicable US NRC requirements and guidelines, such as US NRC GDC 64 and Regulatory Guide 1.21. | | |
|  |  | **Requirement 82: Means of radiation monitoring (cont.)** | | * Exhausts to the environment from the personnel areas in the annex building, electrical and mechanical equipment rooms in the annex and auxiliary buildings, and the diesel generator rooms will not be radioactive because they contain no radioactive materials. These ventilation exhausts are not monitored.   Operation of the PMS following a DEC and Severe accidents is addressed in the **AP1000** plant PRA. | | |
| 6.77 | 1 | Stationary dose rate meters shall be provided for monitoring local radiation dose rates at plant locations that are routinely accessible by operating personnel and where the changes in radiation levels in operational states could be such that access is allowed only for certain specified periods of time. | | The **AP1000** plant design meets this requirement. See **AP1000** plant DCD [2] Section 11.5.  Also see response for Requirement 82 (Power Operation Design Basis). | | |
| 6.78 | 1 | Stationary dose rate meters shall be installed to indicate the general radiation levels at suitable plant locations in accident conditions. The stationary dose rate meters shall provide sufficient information in the control room or at the appropriate control position that operating personnel can initiate corrective action if necessary. | | The **AP1000** plant design meets this requirement. See **AP1000** plant DCD [2] Section 11.5.  Also see response for Requirement 82 (Safety Design Basis). | | |
| 6.79 | 1 | Stationary monitors shall be provided for measuring the activity of radioactive substances in the atmosphere in those areas routinely occupied by operating personnel and where the levels of activity of airborne radioactive substances might be such as to necessitate protective measures. These systems shall provide an indication in the control room or in other appropriate locations when a high activity concentration of radionuclides is detected. Monitors shall also be provided in areas subject to possible contamination as a result of equipment failure or other unusual circumstances. | | The **AP1000** plant design meets this requirement. See **AP1000** plant DCD [2] Section 11.5.  Also see response for Requirement 82 (Power Operation Design Basis). | | |
| 6.80 | 1 | Stationary equipment and laboratory facilities shall be provided for determining, in a timely manner, the concentrations of selected radionuclides in fluid process systems, and in gas and liquid samples taken from plant systems or from the environment, in operational states and in accident conditions. | | The **AP1000** plant design meets this requirement. See **AP1000** plant DCD [2] Section 11.5.  Also see response for Requirement 82 (Power Operation Design Basis & Safety Design Basis). | | |
| 6.81 | 1 | Stationary equipment shall be provided for monitoring radioactive effluents and effluents prior to or during discharges from the plant to the environment. | | The **AP1000** plant design meets this requirement. See **AP1000** plant DCD [2] Section 11.5.  Also see response for Requirement 82 (Power Operation Design Basis). | | |
| 6.82 | 1 | Instruments shall be provided for measuring surface contamination. Stationary monitors (e.g. portal radiation monitors, hand and foot monitors) shall be provided at the main exit points from controlled areas and supervised areas to facilitate the monitoring of operating personnel and equipment. | | The **AP1000** plant design meets this requirement. See **AP1000** plant DCD [2] Section 11.5.  The area radiation monitors are provided to supplement the personnel and area radiation survey provisions of the **AP1000** plant health physics program described in the **AP1000** plant DCD [2] Section 12.5 and to comply with the personnel radiation protection guidelines of 10 CFR 20, 10 CFR 50, and 10 CFR 70; and Regulatory Guides 1.97, 8.2, and 8.8.  During refueling operations in containment and the fuel handling area, criticality monitoring functions, as stated in 10 CFR 70.24, are performed by the area radiation monitors in combination with portable bridge monitors. | | |
| 6.82 (cont.) | 1 |  | | The design objectives of the area radiation monitors during normal operating plant conditions and AOOs are to:   * Measure the radiation intensities in specific areas of **AP1000** plant * Warn of uncontrolled or inadvertent movement of radioactive material in **AP1000** plant * Provide local and remote indication of ambient gamma radiation and local and remote alarms at key points where substantial changes in radiation flux might be of immediate importance to personnel * Annunciate and warn of possible equipment malfunctions and leaks in specific areas of **AP1000** plant * Furnish information for radiation surveys * Minimize the time, effort, and radiation received by operating personnel during routine maintenance and calibration * Incorporate modular design concepts throughout, to provide easy maintenance | | |
| 6.82 (cont.) | 1 |  | | In addition, portable radiation survey instrumentation (**AP1000** plant DCD [2] Section 12.5.2.4, also see response for Paragraph 6.83) is stored at the access control health physics booth and at in-plant control points. This instrumentation allows plant personnel to perform radiation, contamination, and neutron surveys, as needed, as well as collect samples for airborne analysis. Shielded rooms are provided in the health physics area for radioactivity analysis laboratory facilities and for calibration of survey instruments  By meeting the above objectives, the RMS aids health physics personnel in keeping radiation exposures ALARA. | | |
| 6.83 | 1 | Facilities shall be provided for monitoring for exposure and contamination of operating personnel. Processes shall be put in place for assessing and for recording the cumulative doses to workers over time. | | The **AP1000** plant design meets this requirement. See **AP1000** plant DCD [2] Sections 11.5 and 12.5.  In particular the **AP1000** plant DCD [2] Section 12.5 addresses the health physics facilities which are designed with the following objectives:   * Providing capability for administrative control of the activities of plant personnel to limit personnel exposure ALARA and within the guidelines of 10 CFR * Providing capability for administrative control of effluent releases from the plant to maintain the releases ALARA and within the limits of 10 CFR 20 and the plant Technical Specifications. * Providing capability for administrative control of waste shipments from the plant to meet applicable requirements for the shipment and receipt of the material at the storage or burial site.   Access to the radiologically controlled area encompassing the containment and potentially contaminated areas of the annex, auxiliary, and radwaste buildings is normally through the entry/exit area of the health physics section of the annex building. Exit from the radiologically controlled area is at the same location. | | |
| 6.83 (cont.) | 1 |  | | Personnel access to and from the radiologically controlled area is controlled at the health physics booth at the entry/exit points of the health physics area. Logging into the Radiation Permit System and issuance of dosimetry is also handled at this location. The health physics booth is equipped with computer terminals, desks, filing cabinets, and shelves, and other facilities needed for effective control and monitoring of radiation workers in the radiologically controlled area. Workers are logged into a radiation exposure tracking system. The health physics and security log-in functions are integrated. Facilities and equipment are provided at the health physics booth for the following functions:   * Issuing respirators, as needed * Issuing radiation dosimetry, as required * Updating radiation work permits as needed based on information provided by health physics at local control points and at the work locations   The booth has a counter such that the health physics personnel can easily monitor the flow of workers. It is located adjacent to and visible from the health physics pickup and suitup room. | | |
| 6.83 (cont.) | 1 |  | | As radiation workers exit the work areas they go through personnel contamination monitors, shower for decontamination if needed, and receive radiologically controlled first-aid if needed. The health physics area contains the personnel contamination monitoring equipment, decontamination shower facilities, and first-aid equipment.  Health physics includes also the following:  **Whole Body Counting Instrumentation (AP1000** **plant DCD [2] Section 12.5.2.3)**  The whole body counter(s) is located in a low background radiation area in the Annex Building. The whole body counting equipment is capable of detecting fractional body burdens of gamma emitting radionuclides.  **Portable Survey Instrumentation (AP1000 plant DCD [2] Section 12.5.2.4)**  Portable radiation survey instrumentation is stored at the access control health physics booth and at in-plant control points. This instrumentation allows plant personnel to perform radiation, contamination, and neutron surveys, as needed, as well as collect samples for airborne analysis. Shielded rooms are provided in the health physics area for radioactivity analysis laboratory facilities and for calibration of survey instruments | | |
| 6.84 | 1 | Arrangements shall be made to assess exposures and other radiological impacts, if any, in the vicinity of the plant by environmental monitoring of dose rates or activity concentrations, with particular reference to:  (a) Exposure pathways to people, including the food chain;  (b) Radiological impacts, if any, on the local environment;  (c) The possible buildup, and accumulation in the environment, of radioactive substances;  (d) The possibility of there being any unauthorized routes for radioactive releases. | | This requirement is met for the **AP1000** plant as discussed in the **AP1000** plant DCD [2] [2] Sections 12.4.2 and 11.3.3.  The **AP1000** plant DCD [2] Chapter 11 discusses the Radioactive Waste Systems (Liquid, Gaseous & Solid) and the possible release pathways and their control. The **AP1000** plant DCD [2] Chapter 12 discusses the radiological impact.  In addition the **AP1000** plant ER [6], developed for the UK GDA, extensively addresses the environmental impacts of the **AP1000** plant (both human and non-human doses assessment) and monitoring measures:  There are six types of environmental monitoring programs that are typically used in the **AP1000** plant system, as described below:   1. **Radiological Monitoring**  * Collection of environmental samples (from air, water, sediment, fish and food products, as well as direct radiation levels) to determine the concentrations of radioactive constituents in the samples. * Monitoring of annual total dose contributions to the maximum exposed individual from radioactive emissions and other nearby radioactive sources. * Monitoring of on-site worker and off-site populations on a regular basis to ensure that exposures to radioactive are within limits. | | |
| 6.84 (cont.) | 1 |  | | 1. **Hydrological Monitoring**  * Periodic monitoring and subsequent sediment removal for maintenance from the cooling water system intake channel to minimize any impact to the raw water system operation. * Bathymetric survey of the intake channel is expected after first year of operation to measure sediment build up and also to determine future dredging intervals. * Monitoring of surface water and groundwater parameters are expected quarterly for the first year of operation, then annually. * Operational monitoring concentrates on parameters are below:   + Surface water flow   + Groundwater flow   + Impact of sanitary and chemical waste retention methods on water quality   + Sediment transport   + Floodplain and wetlands  1. **Ecological Monitoring**  * Procedures to monitor terrestrial species and habitats that could be adversely affected. * Sampling and monitoring procedures on fish and aquatic species, and habitats that could be adversely affected by the intake or discharge of cooling water or other operational impacts. | | |
| 6.84 (cont.) | 1 |  | | 1. **Thermal Monitoring**  * Routine thermal monitoring of waste water discharges (specifically outfall, blow down, and electric power generation discharges).  1. **Chemical Monitoring**  * Monitoring of discharges made through outfall for consistency. * Monitoring of physical, biological, and chemical attributes. * Monitoring of tanks containing oil or hazardous substances during tank filling operations. * Monitoring procedures of continuous leak detection systems. * Inspections to verify that hazardous waste is treated, stored, and disposed of.  1. **Meteorological Monitoring**  * Collection and monitoring of data on-site conditions which includes wind speed and direction, dry-bulb temperature, dew point temperature, and rainfall. | | |