F-APP-GW-GAP-061-1, Rev. 3

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DOCUMENT COVER SHEET** | | | | | |  | | | |
| DOCUMENT NO. | | | REVISION | | PAGE | | | OPEN ITEMS | |
| APP-GW-G0R-014 | | | A | | 1 of 194  PE Stamp (if required) | | |  | |
| DOCUMENT STATUS: | | | **AP1000** SAFETY CLASS: **N/A** | | | | |  | |
| LICENSING REVIEW STATUS: | | | | | | | |  |  | |
| SEISMIC CATEGORY: N/A | | | | | | | |  |  | |
| APPLICABILITY ASSESSMENT: | | | | | | | |  |  | |
| Applies to the following plants: | | | | | | | |  |  | |
| FTR | | | | | | | |  |  | |
|  | |
| ALTERNATE DOCUMENT NUMBER: N/A | | | | | | | |  | |
| TITLE: | | Assessment of the AP1000 Plant to IAEA Specific Safety Guide No. SSG-64 "Protection against Internal Hazards in the Design of Nuclear Power Plants” | | | | | |  | |
| DCP/ADL/EDCR# INCORPORATED AND/OR MINOR REVISION # RECONCILED IN THIS DOCUMENT REVISION:  N/A | | | | | | | |  | |
| ATTACHMENTS: N/A | | | ADL ATTACHED | | | | PRE E&DCR Issued for this Direct Revision  PRE E&DCR:      N/A | | |
| PARENT DOCUMENT:      N/A | | | | | | | | | |
|  | | **© 2023 WESTINGHOUSE ELECTRIC COMPANY LLC, ALL RIGHTS RESERVED – WESTINGHOUSE NON-PROPRIETARY CLASS 3**  All Class 3 Documents require the following two approvals in lieu of a Form 36. | | | | | | | | |
|  | | LEGAL REVIEW | | | | | | SIGNATURE / DATE **(If processing electronic approval select option)** | | |
|  | | PATENT REVIEW | | | | | | SIGNATURE / DATE | | |
|  | | **© 2023 WESTINGHOUSE ELECTRIC COMPANY LLC, ALL RIGHTS RESERVED – WESTINGHOUSE PROPRIETARY CLASS 2** | | | | | | | | |
|  | | Information included in this material is proprietary and confidential and cannot be disclosed or used for any reason beyond the intended purpose without the prior written consent of Westinghouse Electric Company LLC.  **\*NOTE: This selection is only to be used for Westinghouse generated documents.** | | | | | | | | |
|  | | **© 2023 WESTINGHOUSE ELECTRIC COMPANY LLC, ALL RIGHTS RESERVED and/or © 2023 WESTINGHOUSE AP1000 BUSINESS PARTNER, ALL RIGHTS RESERVED WESTINGHOUSE PROPRIETARY CLASS 2 and/or WESTINGHOUSE BUSINESS PARTNER PROPRIETARY (SEE ATTACHED DOCUMENT)** | | | | | | | | |
|  | | Information included in this material is proprietary and confidential and cannot be disclosed or used for any reason beyond the intended purpose without the prior written consent of Westinghouse Electric Company LLC. | | | | | | | | |
|  | | **SUPPLIER OR THIRD PARTY PROVIDED INFORMATION – File And Protect Using Policies For Westinghouse Proprietary Class 2 Information**  Information included in this material is proprietary and confidential and cannot be disclosed or used for any reason beyond the intended purpose without the prior written consent of the Supplier/Third Party. | | | | | | | | |
| ORIGINATOR(S)  Mikolaj Brzezinski | | | | SIGNATURE / DATE **(If processing electronic approval select option)** | | | | | |
| REVIEWER(S)  Julie Gorgemans | | | | SIGNATURE / DATE | | | | | |
|  | | | | SIGNATURE / DATE | | | | | |
|  | | | | SIGNATURE / DATE | | | | | |
| VERIFIER(S)  N/A | | | | SIGNATURE / DATE | | | Verification Method: **N/A** | | |
|  | | |
| RESPONSIBLE MANAGER\*  Russell L Porterfield | | | | SIGNATURE / DATE | | | | | |
| *\*Approval of the responsible manager signifies that the document and all required reviews are complete, the appropriate proprietary class has been assigned, electronic file has been provided to PRIME, and the document is released for use.*  *This document may contain technical data subject to the export control laws of the United States. In the event that this document does contain such information, the Recipient’s acceptance of this document constitutes agreement that this information in document form (or any other medium), including any attachments and exhibits hereto, shall not be exported, released or disclosed to foreign persons whether in the United States or abroad by recipient except in compliance with all U.S. export control regulations. Recipient shall include this notice with any reproduced or excerpted portion of this document or any document derived from, based on, incorporating, using or relying on the information contained in this document.* | | | | | | | | | |

APP-GW- G0R-014  
Revision A

Assessment of the AP1000 Plant to IAEA Specific Safety Guide No. SSG-64 "Protection against Internal Hazards in the Design of Nuclear Power Plants”

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. Other names may be trademarks of their respective owners.

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

RECORD OF CHANGES

| Revision | Author | Description | Completed |
| --- | --- | --- | --- |
| A | Mikolaj Brzezinski | Original Issue  Licensing review of preliminary “alpha” documents is not required, per Appendix C of APP-GW-GAP-147, Revision 17 | See PRIME |
|  |  |  |  |

OPEN ITEMS

| Item | Description | Status |
| --- | --- | --- |
| N/A | No open items |  |

TABLE OF CONTENTS

[1 INTRODUCTION 1-1](#_Toc144456713)

[1.1 OVERVIEW AND PURPOSE OF DOCUMENT 1-1](#_Toc144456714)

[1.2 STANDARD AP1000 PLANT AS BASIS FOR THE ASSESSMENT 1-1](#_Toc144456715)

[1.3 APPLICATION OF THE GUIDE TO THE AP1000 PLANT 1-2](#_Toc144456716)

[1.4 AP1000 PLANT DESCRIPTION APPLICABLE TO THE GUIDE 1-3](#_Toc144456717)

[1.4.1 OVERVIEW 1-3](#_Toc144456718)

[1.4.2 AP1000 PLANT DESIGN FOR INTERNAL HAZARDS 1-4](#_Toc144456719)

[1.4.3 OVERVIEW OF THE AP1000 PLANT FIRE PROTECTION SYSTEM 1-5](#_Toc144456720)

[1.4.4 PROTECTION FROM INTERNAL FLOODING 1-7](#_Toc144456721)

[1.4.5 PRESSURE PART FAILURE 1-8](#_Toc144456722)

[1.4.6 INTERNALLY GENERATED MISSILES 1-11](#_Toc144456723)

[1.4.7 SEISMIC INTERACTION 1-12](#_Toc144456724)

[2 DETAILED ASSESMENT ASSESSMENT OF GUIDE CLAUSES AND REQUIREMENTS 2-1](#_Toc144456725)

[2.1 GUIDE ARTICLES/SUBARTICLES COMPLIANCE ASSESSMENT CATEGORIES 2-1](#_Toc144456726)

[2.2 GENERAL CONSIDERATIONS 2-2](#_Toc144456727)

[2.3 GENERAL DESIGN RECOMMENDATIONS FOR PROTECTION AGAINST INTERNAL HAZARDS 2-7](#_Toc144456728)

[2.4 RECOMMENDATIONS FOR SPECIFIC INTERNAL HAZARDS 2-24](#_Toc144456729)

[2.5. APPENDIX I – HAZARD COMBINATIONS 2-133](#_Toc144456730)

[2.6. APPENDIX II - DETAILED GUIDANCE ON INTERNAL FIRES 2-139](#_Toc144456731)

[3 SUMMARY AND CONCLUSIONS 3-1](#_Toc144456732)

[3.1 IDENTIFIED POTENTIAL RISKS TO BE ADDRESSED IN FUTURE PROJECT 3-1](#_Toc144456733)

[3.2 NON-COMPLIANCES 3-1](#_Toc144456734)

[4 REFERENCES 4-1](#_Toc144456735)

LIST OF ACRONYMS AND ABBREVIATIONS

|  |  |
| --- | --- |
| AC | Alternating Current |
| ALARA | As Low As Reasonably Achievable |
| ALARP | As Low As Reasonably Practicable |
| ANS | American National Standards |
| ANSI | American National Standards Institute |
| ASME | American Society of Mechanical Engineers |
| ATWS | Anticipated Transients without Scram |
| BEZ | Break Preclusion Zone |
| BSO | Basic Safety Objective |
| BTP | Branch Technical Position |
| CAS | Compressed and Instrument Air System |
| CFR | Code of Federal Regulations |
| COM | Compliant |
| CWO | Compliant with Objective |
| DBA | Design Basis Accident |
| DBE | Design Basis Event |
| DCD | Design Control Document |
| DEC | Design Extension Condition |
| DG | Diesel Generator |
| DID | Defense-In-Depth |
| DOR | Division Of Responsibility |
| EGS | Grounding and Lightning Protection System |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| EMIT | Examination, Maintenance, Inspection and Testing |
| EP | External Party |
| ESD | Electrostatic Discharge |
| EU | European Union |
| FPS | Fire Protection System |
| GDC | General Design Criterion |
| HVAC | Heating, Ventilating and Air Conditioning |
| I&C | Instrumentation and Control |
| IAEA | International Atomic Energy Agency |
| IEEE | Institute of Electrical and Electronics Engineers |
| LBB | Leak Before Break |
| LFL | Lower Flammable Limit |
| LLW | Low Level Waste |
| LLWR | Low-Level Waste Repository |
| LOCA | Loss-Of-Coolant Accident |
| MCR | Main Control Room |
| N/A | Not Applicable |
| NAS | Not Assessable |
| NFPA | National Fire Protection Association |
| NI | Nuclear Island |
| NOC | Non-Compliant |
| NR | Not a Requirement |
| NRC | Nuclear Regulatory Commission |
| OR | Owner Requirement |
| PAR | Passive Autocatalytic Recombiner |
| PCCWST | Passive Containment Cooling Water Storage Tank |
| PGS | Plant Gas System |
| PMS | Protection and Safety Monitoring System |
| POS | Project or Site-specific Scope |
| PRA | Probabilistic Risk Assessment |
| PSA | Probabilistic Safety Assessment |
| PWR | Pressurized Water Reactor |
| QA | Quality Assurance |
| RCP | Reactor Coolant Pump |
| RCS | Reactor Coolant System |
| RG | Regulatory Guide |
| RSR | Remote Shutdown Room |
| SCBA | Self-Contained Breathing Apparatus |
| SEE | Safe Shutdown Earthquake |
| SF | Spent Fuel |
| SFP | Spent Fuel Pool |
| SSC | Structures, Systems, and Components |
| TWC | Through Wall Crack |
| UK | United Kingdom |
| US | United States |
| VBS | Island Nonradioactive Ventilation System |
| VES | Main Control Room Emergency Habitability System |
| WLS | Liquid Radwaste System |
| WRS | Radioactive Waste Drain System |
| WWS | Waste Water System |

# INTRODUCTION

## OVERVIEW AND PURPOSE OF DOCUMENT

This document provides a compliance assessment of the standard AP1000 plant design to the following IAEA safety guide:

* IAEA Safety Standards Series No. SSG-64 Protection against Internal Hazards in the Design of Nuclear Power Plants [1].

This IAEA Specific Safety Guide (SSG) [1] is herein referred to as the “Guide”.

## STANDARD AP1000 PLANT AS BASIS FOR THE ASSESSMENT

The standard AP1000 plant design is the design documented in APP-GW-GL-700 Rev. 19, “AP1000 Plant Design Control Document” [2], herein referred to as the Design Control Document (DCD [2]). This standard AP1000 plant design is used as the basis for the assessment as it provides one consistent reference document with sufficient documentation to demonstrate the safety approach for the AP1000 plant design, analysis, and licensing basis in the United States.

The Reference Plant design for future AP1000 units is the Vogtle Unit 4 design. The Final Safety Analysis Report of this AP1000 unit is publicly available in reference [3]. Design and licensing updates have occurred for the Vogtle Unit 4 design since the issuance of the DCD [2]. However, the DCD [2] provides documentation that supports the safety approach of the AP1000 plant design for the Reference Plant and future AP1000 plant designs for the purpose of demonstrating compliance or assessing the potential risks for a project related with regulations, guides, codes and standards, that could potentially be used in the project at a later stage.

A probabilistic safety assessment (PSA) consists of a systematic and comprehensive evaluation of the risks. This exercise is referred to as ‘probabilistic risk assessment’ in the U.S. regulatory terminology. These two names are equivalent. The design Probabilistic Risk Assessment (PRA) for the standard AP1000 plant is documented in APP-GW-GL-022 Rev. 8 [4]. The design PRA [4] provides a basis to demonstrate the PRA approach and methodology implemented in informing the standard AP1000 plant design documented in the DCD [2]. For the Reference Plant, there is a Vogtle Unit 3 & 4 specific PRA that has been developed implementing updates to the AP1000 plant design from the standard AP1000 plant design to the Vogtle Unit 4 design and site-specific aspects of the Vogtle 3 & 4 AP1000 units, based on the design PRA. The design PRA [4] is used in this compliance assessment to provide consistent documentation to the DCD [2] and because it adequately demonstrates the PRA methodology and PRA basis for the overall AP1000 plant design. For the future AP1000 plant project, the updated Vogtle Unit 3&4 PRA will be the basis for the future PRA as Vogtle Unit 4 will be the Reference Plant.

This document contains a preliminary compliance/risk assessment performed primarily to the standard AP1000 plant design documented in APP-GW-GL-700 Rev. 19, with review of any Reference Plant (Vogtle 4) licensing basis design changes (as of the date of this document) that would impact the assessment of compliance.

A final reconcilation and compliance assessment will be required to be performed after finalization of the Reference Plant (Vogtle 4) design and licensing basis and incorporation of design changes implemented for anyAP1000 plant project and any new analyses that may need to be performed for a specific AP1000 to address final compliance with the Regulation [1].

## APPLICATION OF THE GUIDE TO THE AP1000 PLANT

The Guide [1] is applicable to the following AP1000 plant design, analysis, and licensing aspects:

* Site-specific hazards, explosion by on-site storage facilities, flammable vapor clouds by on-site flammable liquids or gases described in DCD Section 2.2,
* Release of hazardous substances described in DCD Chapter 2.2 and Chapter 11,
* Collapse of structures and falling objects described in DCD Chapter 3 and Chapter 9,
* Internal Flooding described in DCD Section 3.4 and Section 19.56,
* Missiles Protection described in DCD Section 3.5,
* Protection Against the Dynamic Effects Associated with the Postulated Rupture of Piping described in DCD Section 3.6,
* Leak-before-break criteria for AP1000 plant piping described in DCD Appendix 3B,
* Methodology for Qualifying AP1000 Safety-Related Electrical and Mechanical Equipment described in DCD Appendix 3D,
* Electrical Disturbances and Electromagnetic Interferences described in DCD Chapter 7 and Chapter 8,
* Heavy load-drop described in DCD Section 9.1.5,
* Fire Protection System described in DCD Section 9.5.1,
* Fire Protection Analysis described in DCD Appendix 9A,
* Human factors described in DCD Chapter 15 and Chapter 18,
* Internal Flooding Analysis described in PRA Chapter 56,
* Fire Risk Assessment described in PRA Chapter 57.

In particular, the following Chapters and Appendices of the Guide [1] contain requirements related to plant design:

* Chapter Two – General Considerations,
* Chapter Three – General Design Recommendations for Protection Against Internal Hazards,
* Chapter Four – Recommendations for Specific Internal Hazards,
* Appendix I – Hazard Combinations,
* Appendix II – Detailed Guidance on Internal Fires.

The following Chapters are excluded from the assessment as they have no impact on the design of the New Nuclear Power Units: Chapter One – Introduction.

## AP1000 PLANT DESCRIPTION APPLICABLE TO THE GUIDE

### OVERVIEW

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). 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. It 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. The AP1000 plant design also 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 (SFP) integrity, and spent fuel cooling. 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.

In addition to redundancy, passive safety features and extensive plant simplifications 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 PRA targets. The passive features are classified as safety in the U.S. The active DiD features are classified as AP1000 plant Class D, e.g. as non-safety (with supplemental requirements) in the U.S. The AP1000 plant Class D corresponds to lower tier safety classes in European classification scheme (for example, United Kingdom (UK) safety class 2, European Utility Requirements (EUR) F2 functions) and meets the relevant design and quality assurance (QA) requirements.

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 passive safety features. 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. 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; and 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.

### AP1000 PLANT DESIGN FOR INTERNAL HAZARDS

Internal Hazards are defined as natural or man-made hazards that originate within the controlled site and its processes as potentially influencing safety-related functions. AP1000 plant is designed to protect against the range of internal hazards identified in SSG-64 Safety Guide [1]. The plant is designed to protect against such internal hazards as internally generated missiles, pipe failures, pipe whip, jet effects, flooding, explosions, fires, collapse of structures and falling objects, electromagnetic interferences, and release of hazardous substances. Operation of the AP1000 plant is tolerant to faults as the passive design significantly improves the response of the plant with appreciably reduced risk to the public, workforce, and environment. As a consequence of this design, AP1000 operations do not result in:

* Loss of control of core reactivity
* Loss of control of removal of heat from the core
* Uncontrolled exposure of plant personnel or the public to radiation
* Uncontrolled dispersion of radioactivity

The safety approach for internal hazards consists in the combination of three different strategies:

* Prevention of the internal hazard fault,
* Protection from the internal hazard fault (incorporation of protective measures in the design to safeguard safety-related SSCs from the effects of an internal hazard),
* Mitigation of the internal hazard fault (through the action of non-affecting SSCs, selection of materials, limiting inventories, or use of redundant divisions).

There are a number of important conservative attributes which have been applied universally to all internal hazards assessments within the AP1000 safety report. These attributes are used to define both the fundamental assessment approach and to establish the degree of safety margin relative to a realistic assessment of the internal hazards fault. In brief, these conservatisms are represented as:

* All internal hazards assessments within the AP1000 safety case are performed from a deterministic perspective. Hazards have not been excluded from consideration based on their hazard curve frequency of exceedance as below once in ten million years. This attribute conservatively addressed the explicit occurrence of an internal hazard faults without filtering the lower probability faults, thus creating a broader base of initiating events in assessing the internal hazard. In addition to the deterministic assessment, internal hazards have also been assessed from a realistic probabilistically perspective within the AP1000 Probabilistic Risk Assessment [4].
* Each of the internal hazards assessments focus on the use of unmitigated consequences as a basis for the analyses acceptance. In this manner, use of conservative assumptions as applicable to these consequences is used consistently throughout the internal hazards assessments in determining an acceptable result.
* Operator actions have been minimized in so far as possible as mitigation responses in all internal hazard assessments. In the few areas where such actions are required, cross cutting inputs and reviews from the Human Factors area, including consideration of human errors, have been used to assess viability of the action and suitability of the time required.
* Analysis of internal hazard faults assume the event occurs simultaneously with the facility’s most adverse permitted operating state.
* Single failure has been applied throughout the internal hazards assessments.

### OVERVIEW OF THE AP1000 PLANT FIRE PROTECTION SYSTEM

The primary objectives of the AP1000 plant fire protection program are to prevent fires and to minimize the consequences should a fire occur. The program provides protection so that the plant can be shut down safely following a fire. The FPS detects and suppresses fires and is an integral part of the AP1000 plant fire protection program.

The FPS was designed with consideration of NUREG-0800, U. S. Nuclear Regulatory Commission Standard Review Plan, Section 9.5.1, “Fire Protection Program,” including Branch Technical Position (BTP) CMEB 9.5-1, “Guidelines for Fire Protection for Nuclear Power Plants,” [5]. Compliance with the BTP is assessed in DCD Table 9.5.1-1 [2].

**Design Basis**

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 main control room (MCR), should a fire require evacuation of the MCR or damage the MCR circuitry for safe shutdown systems.
* Separate redundant trains of safety-related equipment used to mitigate the consequences of a design basis accident (but not required for safe shutdown following a fire) 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 FPS 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-related equipment.
* Provide firefighting personnel access and life safety escape routes for each fire area.
* 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.

As active fire suppression is not necessary for the safe shutdown of the plant following a fire, the FPS is classified as a nonsafety-related, non-seismic system. Special seismic design requirements are applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake, as described in DCD subsection 9.5.1.2.1.5 [2]. In addition, the containment isolation valves and associated piping for the FPS are safety related (Safety Class 2) and Seismic Category I. The FPS is not required to remain functional following a plant accident or the most severe natural phenomena, except as indicated below for a safe shutdown earthquake.

The FPS is designed to perform the following functions:

* Detect and locate fires and provide operator indication of the location.
* 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 (114 m3/hr) 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.
* Satisfy the requirements of the passive containment cooling system as an alternate source of water to wet the containment dome or to refill the passive containment cooling water storage tank after a loss-of-coolant accident if the FPS is available.
* Provide an alternate supply of cooling water to the normal residual heat removal system heat exchanger after a loss of normal component cooling water system function.
* Provide non-safety-related containment spray capability for severe accident management.

**System Description**

The plant includes features to minimize the likelihood that a fire will occur and to limit the spread of fire. The FPS detects fires and provides the capability to extinguish them using fixed automatic and manual suppression systems, manual hose streams, and/or portable firefighting equipment. The FPS consists of a number of fire detection and suppression subsystems, referred to as systems, including:

* Detection systems for early detection and notification of a fire.
* A water supply system including the fire pumps, yard main, and interior distribution piping.
* Fixed automatic fire suppression systems.
* Manual fire suppression systems and equipment, including hydrants, standpipes, hose stations and portable fire extinguishers.

Additional details on the FPS and fire protection analysis are provided in DCD subsection 9.5.1 and Appendix 9A [2].

### PROTECTION FROM INTERNAL FLOODING

The AP1000 plant arrangement provides physical separation of redundant safety-related components and systems from each other and from nonsafety-related components. As a result, component failures resulting from internal flooding do not prevent safe shutdown of the plant or prevent mitigation of the flooding event. Protection mechanisms are described DCD in Section 3.6 [2]. The protection mechanisms related to minimizing the consequences of internal flooding include the following:

* Structural enclosures
* Structural barriers
* Curbs and elevated thresholds
* Leak detection systems
* Drain systems

The AP1000 plant minimizes the number of penetrations through enclosure or barrier walls below the flood level. Those few penetrations through flood protection walls that are below the maximum flood level are watertight. Any process piping penetrating below the maximum flood level either is embedded in the wall or floor or is welded to a steel sleeve embedded in the wall or floor. There are no watertight doors in the AP1000 plant used for internal flood protection because, as described in DCD subsection 3.4.1.2.2 [2], they are not needed to protect safe shutdown components from the effects of internal flooding. The walls, floors, and penetrations are designed to withstand the maximum anticipated hydrodynamic loads associated with a pipe failure as described in DCD Section 3.6 [2]. The two watertight doors on the waste holdup tank compartments limit the consequence of a failure on spent fuel pool water level.

Each area of the plant containing safety-related systems or equipment is reviewed to determine the postulated fluid system failures which would result in the most adverse internal flooding conditions. For the internal flooding analysis, the failure of safety-related systems, structures or components is acceptable provided they have no safe shutdown function, or the safe shutdown function is otherwise accomplished. The internal flooding analysis shows that SSCs are not prevented from performing their required safe shutdown functions due to the effects of the postulated failure. In addition, the analysis identifies the protection features that mitigate the consequences of flooding in an area that contains safety-related equipment. The flooding sources considered in the analysis consist of the following:

* High-energy piping (breaks and cracks)
* Through-wall cracks in seismically-supported moderate energy piping
* Breaks and through-wall cracks in non-seismically-supported moderate energy piping
* Pump mechanical seal failures
* Storage tank ruptures
* Actuation of fire suppression systems
* Flow from upper elevations and adjacent areas

The analysis is performed based on the criteria and assumptions provided in DCD Section 3.6 [2] and ANS-56.11 [6]. Section 3.6 in DCD [2] provides the criteria used to define break and crack locations and configurations for high and moderate-energy piping failures. The analysis consists of the following steps:

* Identification of the flood sources
* Identification of essential equipment in area
* Determination of flowrates and flood levels
* Evaluation of effects on essential equipment

The analysis of potential flooding events is performed on a floor-by-floor and room-by-room basis depending upon the relative location of safety-related equipment. No credit is taken for operation of sump pumps to mitigate the consequences of flooding. The analysis focusing on flooding events in the auxiliary building and containment since this is the safety related footprint for the design. The analysis demonstrates that the plant design protects against effects of internal flooding such that no credible flooding source can prevent safety shutdown.

### PRESSURE PART FAILURE

Pressure part failures in piping are internal hazards defined as full area gross failures, such as double ended and longitudinal breaks, as well as cracks in piping, such as through wall cracks (TWC), and Leak Before Break (LBB) leakage cracks. Only one pressure part failure is postulated as an initiating event, but consequential failures in adjacent pipes are evaluated if cascading events are determined per pre-defined interaction criteria. The evaluated areas of the pipe hazards includes dynamic effects including jet impingement, pipe whip, subcompartment pressurization, fluid system decompression, as well as spray wetting and flooding from pipe failure. High energy and moderate energy lines are defined by pressure and temperature criteria. The systems, structures, and components that have a required function in the adverse environmental conditions including temperature, humidity, pressure, and chemical consequences, are also evaluated.

In demonstrating a safe plant consideration, to the extent possible, layout options are pursued to minimize the occurrences where potential essential SSCs are in proximity to the piping failure hazard.

The AP1000 plant piping failure protection program is generally in compliance with 10 CFR 50 Appendix A, General Design Criterion 4, ANS-58.2-1988, Standard Review Plan Section 3.6.1, 3.6.2, and NUREG-1061 Volume 3. Key elements of the AP1000 plant pipe failure protection program are summarized below.

**Break Preclusion with Break Exclusion Zones**

Break exclusion zones (BEZ) are portions of pipe in containment penetration areas where consideration of dynamic effects initiating pipe pressure part failures are excluded, demonstrated using increased stress limits and criteria, except for select cases of compartment pressurization analysis.

**Break Preclusion with Mechanistic Pipe Rupture Concepts**

High energy piping of nominal pipe size greater than 150 mm DN (6 inches) are qualified to mechanistic pipe failure considerations, using leak-before-break (LBB) methodology, and are precluded from dynamic effects considerations. Mitigation for the effects of LBB piping rely on the detection of those leakage, and analysis is performed to demonstrate stability as well as leakage crack size to the required extent to that the leak can be properly detected. For these LBB sections of pipe, only evaluated for the effects of leakage cracks, of which the resulting harsh environments are evaluated on the qualification of equipment.

**Evaluation of Dynamic Effects**

Pipe break locations are generally determined using considerations of translational and rotational rigidity such as in the case of 6 way anchors. Additionally, pipe breaks are postulated at pressurized ends of closed valves, locations of high stress and thermal fatigue, and also determined based on seismic classification. Enveloping zones are developed that represent affected volumes of the whipping pipe, fluid jet, and resulting missiles are put into the plant 3-D model for special assessment. Additionally, the piping system containing the pipe rupture is also assessed. Safety-related systems, structures, and components that are in the break-affected zone are identified and further determinations are made whether those particular safety related items are essential, considering plant redundancies as well as limiting single failure criterion. In the event of a high- or moderate-energy pipe failure within the plant, adequate protection is provided so that essential structures, systems, or components are not impacted by the adverse effects of postulated piping failure. Essential systems and components are those required to shut down the reactor, maintain a safe shutdown condition, and mitigate the consequences of the postulated piping failure. No-essential system structures and components are evaluated if their failures lead to failure of and essential system. Hazards from pipe failure that are found to affect essential systems, structures, and components are either separated by distance, separated from break-affected zone with a protective device, qualified by analysis, protected by mitigating inline systems or components, or any combination of those. Protective devices mitigate the break effects by physical restraining the pipe with a pipe whip restraint or physical barrier, or by shielding and essential SSC from the fluid jet expelled from the failed pipe with a jet impingement shield or guard pipe. In addition to protecting essential SSCs, pipe failure effects are shown to not preclude access to areas that are required to recover from the postulated failure, nor habitability of the main control room.

Safety related structures bounding compartments with pipe breaks are qualified to withstand the dynamic asymmetric compartment pressurization of the associated pipe failure. Compartment pressures are calculated using mass and energy release data produced for the postulated pipe failure.

**Environmental Qualification**

Essential portions of safety-related systems structure and components are demonstrated as being protected from the effects of harsh environments (spray wetting, humidity, chemical considerations, radiation, different thermal considerations) resulting from the pipe failure.

**Flooding**

Hydrostatic loads on structures as well as operability analysis of submerged essential components are evaluated for the effects of flooding caused by piping failure.

**Internal System Depressurization**

Dynamic pressure waves inside the broken piping system are evaluated on essential inline components as well as the structural integrity of essential portions of the piping system. Check valves are also checked in detail for dynamic effects caused by rapid closures resulting from depressurization of the system.

**Mitigating Devices**

The non-energy absorbing portions of pipe whip restraints, guard pipes, and jet impingement shields, which are intended to arrest the broken whipping pipe as well as modify the break affected zones, are designed and qualified per the requirements of AISC-N690 code. Energy absorbing features on these mitigating devices such as elongating U-bars and crushable materials, are designed based on energy absorption principles considering elastic-plastic, strain hardening behavior of the material used.

**Loads Considerations**

Loads (forces, moments, and energies) on essential systems, structures, and components as well as load paths credited as necessary in to mitigating the break effects are considered using the governing codes and standards of the affected commodity. Only qualification on systems, structures, and components that are needed to demonstrate a safe plant condition are considered.

### INTERNALLY GENERATED MISSILES

The plant is designed to protect against internally generated missiles. The plant is designed to meet U.S. NRC General Design Criteria 4 of Appendix A to 10 CFR 50 that requires SSCs important to safety to be protected from the effects of missiles. The AP1000 plant criteria for protection from postulated missiles provide the capability to safely shutdown the reactor and maintain it in a safe shutdown condition. The plant design criteria also require that protection of the reactor coolant pressure boundary integrity be maintained. The plant’s design to eliminate and protect against internally generated missiles is described in detail in DCD Chapter 3.5 [2]. The information below provides a summary of the designs approach for internally generated missiles.

Internally missiles may be generated by pressurized components, rotating machinery, and explosions within the plant. Potential missile hazards are eliminated to the extent practical by minimizing the potential sources of missiles through proper selection of equipment, and by arrangement of structures and equipment in a manner to minimize the potential for damage from missiles. Potential missiles due to failures of non-seismic items are addressed in DCD Chapter 3.7.3.13 [2], and heavy load-drop evaluations are described in DCD Chapter 9.1.5 [2].

Evaluations are performed to the demonstrate the criteria defined above are satisfied in the event a credible missile is produced coincident with a single active component failure. The evaluations include the following:

* For those potential missiles considered to be credible, a realistic assessment is made of the postulated missile size and energy, and its potential trajectories.
* Potentially impacted components associated with systems required to achieve and maintain safe shutdown are identified.
* Loss of these potentially impacted components coincident with an assumed single active component failure is evaluated to determine if sufficient redundancy remains to achieve and maintain a safe shutdown condition. If these criteria are satisfied, further protection is required for the identified missile. If these conditions are not satisfied, additional protective features are incorporated (for example, plant layout is modified, or barriers are added).

Credible missiles are identified and evaluated both inside and outside of containment. The criteria for identifying credible missiles are defined in DCD Chapter 3.5.1.1.2 [2]. Specific components are designed and evaluated to demonstrate that missile generation is either non-credible or any potential failure would be contained within the casing of the component. Specifically, the reactor coolant pump design requirements are established so that any failure of the rotating parts would be retained within the casing at the specified overspeed conditions. Gross failure of other components such as the reactor vessel, steam generator, pressurizer, core makeup tanks, accumulators, reactor coolant pump casings, passive residual heat removal heat exchanger, and piping leading to the generation of missiles is not considered credible due to material characteristics, pre-service and in-service inspections, quality control during fabrication, and other defined preventative measures.

**Turbine Missiles**

The turbine generator is located north (generic plant north is towards the turbine building) of the nuclear island with its shaft oriented north-south. In this orientation, the potential for damage from turbine missiles is negligible. Safety-related structures, systems and components are located outside the high-velocity, low-trajectory missile strike zone. Thus, postulated low-trajectory missiles cannot directly strike safety-related areas.

The turbine and rotor design provides for missile protection due to the orientation of the turbine-generator and by the use of robust turbine rotors. The rotor design, manufacturing, and material specification and the inspections recommended for the AP1000 plant provide an acceptably very low probability of missile generation. This low probability computation includes fatigue and fracture analysis, material selection, and the maintenance program requirements.

The potential for a high-trajectory missile to impact safety-related areas of the AP1000 plant is less than 10-7. Based on this very low probability of an impact in the safety-related areas is the product of the probability of missile generation from the turbine; the probability, assuming a turbine failure, that a high-trajectory missile would land within a few hundred meters form the turbine (10-6 per square meter); and the area of the safety-related area. In the AP1000 design, the safety-related area is contained within the containment shield building and the auxiliary building.

### SEISMIC INTERACTION

SSCs are assigned a seismic category of either C-1, C-II, or NS. SSCs required to protect the plant in the event of a safe shutdown earthquake (SSE) are designed as C-I, which means that the components will maintain both its integrity and functionality following a seismic event up to the defined SSE of 0,3g. Additional evaluations and design features are incorporated to prevent adverse seismic interaction between the C-I SSCs and the C-II and NS SSCs. The plant design requires that the safety functions of C-I SSCs are either protected from interaction with NS SSCs or their interaction is evaluated and shown to be acceptable.

The plant’s design criteria for protection against adverse seismic interaction are described in more details in DCD Chapter 3.7.3.13 [2]. The primary means of protection safety related SSCs from adverse interaction are outlined below:

* Separation – Separation with the use of physical barriers.
* Segregation – Routing away from location of C-I SSCs.
* Impact Evaluation – Contact with C-I SSCs may occur, and there is insufficient energy in the impact to cause a loss of safety function.
* Support as seismic Category II – NS SSCs that evaluations demonstrate could adversely interact with C-I SSCs are supported as C-II SSCs to prevent the potential adverse interaction.

# DETAILED ASSESMENT ASSESSMENT OF GUIDE CLAUSES AND REQUIREMENTS

This section provides the detailed assessment of the standard AP1000 plant design against the analyzed parts of the IAEA Protection against Internal Hazards in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-64 [1]. Compliance is assessed by the compliance assessment categories identified in Section 2.1 and a justification is provided to support the compliance assessment.

## GUIDE ARTICLES/SUBARTICLES COMPLIANCE ASSESSMENT CATEGORIES

The following compliance categories are applied in the compliance assessment for each of the clauses (sub-articles) of the regulation analyzed in this section:

|  |  |  |
| --- | --- | --- |
| COM | Compliant | Full compliance by Reference Plant design and/or analysis. |
| CWO | Compliant with Objective | The design meets the objectives of the requirement but with an alternate approach than that specifically stated in the requirement. |
| EP | External Party | This requirement is the responsibility of an External Party i.e. Government, Regulatory Body etc. |
| NR | Not a Requirement | Not a design requirement (for example, terms and definitions). |
| NOC | Non-Compliant | Non-compliant: The design does not meet the objective of the requirement. |
| N/A | Not Applicable | Not Applicable: The design is not applicable to the AP1000 plant design, with the justification provided. |
| NAS | Not Assessable | Not Assessable: The requirement is not currently assessable (e.g., unclear requirement, insufficient design maturity, different methodology application than standard AP1000 plant, site-specific feature). |
| OR | Owner Requirement | Owner Requirement that is applicable to the Owner and not fulfilled by the AP1000 plant designer. |
| POS | Project or Site-specific Scope | This requirement requires project or site-specific scope to be performed to meet the requirement.  The responsibility party for this scope will be defined in a project-specific DOR; the scope could be the responsibility of the designer, Owner, or other third party. |

## GENERAL CONSIDERATIONS

| **Section/Paragraph** | **Requirement**  **Note:** The references noted in [] in column “Requirement” do not relate to the reference list in Sections 4.0 of this document but relate to the reference list of the IAEA Specific Safety Guide SSG-64. | **Compliance** | **Justification** |
| --- | --- | --- | --- |
| 2.1 | Requirement 17 of SSR‑2/1 (Rev. 1) [1] states:  “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.” | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  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). |
| 2.2 | Paragraph 5.16 of SSR‑2/1 (Rev. 1) [1] states:  “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.” | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  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. |
| 2.3 | Sections 3 and 4 of this Safety Guide provide general design recommendations and specific design recommendations, respectively, to meet Requirement 17 and the requirements established in para. 5.16 of SSR‑2/1 (Rev. 1) [1] regarding internal hazards. | NR | This is a statement not a requirement.  Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7]. |
| 2.4 | An item important to safety is 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 [2]. In accordance with this definition, and the definition of design extension conditions in SSR‑2/1 (Rev. 1) [1], safety features for design extension conditions are items important to safety. Therefore, safety features for design extension conditions need to be designed or protected against applicable internal hazards. In addition, safety features for design extension conditions could be sources of internal hazards that need to be considered. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  Safety-related SSCs are designed to continue to perform their safety functions in the event of an internal hazard as described in DCD [2] Chapter 3.  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, as demonstrated by the design PRA [4] and summarized in DCD [2] Chapter 19. 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 design includes redundancy and physical separation of components as necessary to fulfill the plant’s safety functions. See compliance to US NRC GDCs 5, 13, 22, 24, 26 [8]. |
| 2.5 | Internal hazards are those hazards to the safety of the nuclear power plant that originate from within the site boundary and are associated with failures of facilities and activities that are under the control of the operating organization. The internal hazards covered in this Safety Guide are listed in para. 1.5. | NR | This is a statement not a requirement. |
| 2.6 | The hazards caused by (or occurring at) other facilities on the same site are also considered to be internal hazards. | NR | This is a statement not a requirement. |
| 2.7 | Internal hazards can also be generated by external hazards (e.g. an earthquake followed by an internal flood, an earthquake causing a fire). | NR | This is a statement not a requirement. |
| 2.8 | Effects induced by internal hazards can also result in cascading effects and induce other internal hazards (e.g. a missile can cause a pipe break and then internal flooding). | NR | This is a statement not a requirement. |
| 2.9 | All credible combinations of hazards (see Appendix I) are also considered within the scope of this Safety Guide. | NR | This is a statement not a requirement. |
| 2.10 | Internal hazards have the potential to induce initiating events, to cause failures of equipment that is necessary to mitigate the consequences of such events and to adversely affect (directly or indirectly) the barriers for the prevention of the release of radioactive material. Internal hazards could, because of their nature, simultaneously challenge more than one level of defence in depth, and increase, for example, the degree of dependency between the originator of initiating events and the failure of mitigation equipment. | COM | See response to Section/Paragraph 2.4. |
| 2.11 | While it might not be practical or possible to prevent an internal hazard from triggering an anticipated operational occurrence, one of the objectives of layout and design of the nuclear power plant is to ensure, to the extent practicable, that internal hazards do not trigger an accident. | COM | The AP1000 plant design provides protection for internal hazards. See responses to Sections/Paragraphs 2.1, 2.2, 2.4. |
| 2.12. | The aim of considering internal hazards in the design of nuclear power plants is to ensure that the fundamental safety functions (see Requirement 4 of SSR‑2/1 (Rev. 1) [1]) are fulfilled in any plant state, and that the plant can be brought to and maintained in a safe state after the occurrence of any credible internal hazard. This implies the following:  (a) Redundant systems are segregated to the extent possible or adequately separated, and protected as necessary, to prevent the loss of the safety function performed by the systems.  (b) The design of individual SSCs is such that design basis accidents, or design extension conditions potentially induced by internal hazards, are avoided to the extent practicable.  (c) The segregation, separation and protection measures implemented are adequate to ensure that the system response described in the analysis of postulated initiating events is not compromised by the effects of the internal hazard.  (d) The design is such that an internal hazard does not lead to a common cause failure between redundant safety systems designed to control design basis accidents, and between these systems and the safety features necessary in the event of design extension conditions with core melting.  (e) An internal hazard occurring elsewhere in the plant does not affect the habitability of the main control room. If the main control room is not habitable, access to, and habitability of the supplementary control room are ensured. In addition, and when necessary, access by plant personnel to equipment in order to perform local actions is possible | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  Provisions included in Requirement 4 of SSR-2/1 [7] are met by the AP1000 plant as presented in the AP1000 plant DCD [2] 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.  a), c), d) The AP1000 plant design includes redundancy and physical separation of components as necessary to fulfill the plant’s safety functions. See response for compliance to US NRC GDCs 5, 13, 22, 24, 26 [8]. 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 those systems. A single failure of a component in a redundant system is not capable of affecting the other redundant components. The plant arrangement provides separation between safety-related and non-safety related systems to preclude adverse interaction between safety-related and non-safety related equipment.  b) See also response to Section/Paragraph 2.4.  e) See responses to Sections/Paragraphs 3.33, 4.50, 4.51, 4.52. |
| 2.13 | In accordance with the concept of defence in depth, the first level of defence in depth provides protection against internal hazards in general by ensuring the high quality and reliability of SSCs, by environmental qualification of these SSCs, by application of the principles of redundancy and diversity, by physical separation and segregation, and by design of appropriate barriers and other protective means. Therefore, design against the effects of internal hazards is an iterative process, integrating the needs of protection against several internal hazards. Proper surveillance and in‑service inspections of SSCs need to be implemented for early detection of the occurrence of an internal hazard (or of signs that can lead to the occurrence of an internal hazard) and implementation of necessary corrective actions to ensure protection against the hazard. Identification of hazards at an early stage in the design is often used as a practical method to identify and eliminate hazards. | COM  POS  OR | The AP1000 plant design considers internal hazards and their effects on SSCs. See responses to Sections/Paragraphs 2.1, 2.2, 2.4, 3.1.  Identification of site-specific hazards is the responsibility of the Owner.  The Owner also shall be responsible for proper surveillance and inspections of the SSC. |

## 

## GENERAL DESIGN RECOMMENDATIONS FOR PROTECTION AGAINST INTERNAL HAZARDS

| **Section/Paragraph** | **Requirement**  **Note:** The references noted in [] in column “Requirement” do not relate to the reference list in Sections 4.0 of this document but relate to the reference list of the IAEA Specific Safety Guide SSG-64. | **Compliance** | **Justification** |
| --- | --- | --- | --- |
| 3.1. | Notwithstanding the measures taken to minimize the likelihood of an internal hazard, such hazards are possible. The capability of the nuclear power plant to withstand internal hazards and to mitigate the effects of postulated initiating events caused by them is required to be an integral part of the design of the plant: see para. 5.16 of SSR‑2/1 (Rev. 1) [1]. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  The AP1000 plant design considers internal hazards as described in DCD [2] Section 2.2, DCD Sections 3.4 through 3.7, DCD Section 9.5.1, DCD Appendix 9A, and DCD Chapter 19. This includes the following internal hazards:   * DCD Section 2.2 – Site-specific hazards, explosion by on-site storage facilities, flammable vapor clouds by on-site flammable liquids or gases * DCD Section 3.4 – Internal Flood * DCD Section 3.5 – Missiles * DCD Section 3.6 - Rupture of Piping * DCD Appendix 3B - Leak before break criteria for AP1000 plant piping * DCD Chapter 7 and Chapter 8 - Electrical disturbances and electromagnetic interferences * DCD Section 9.5.1 – Fire Protection * DCD Appendix 9A – Fire Protection Analysis * DCD Section 2.2 and Chapter 11 - Release of hazardous substances * PRA Internal Flood – PRA [4] Chapter 56 * PRA Internal Fire – PRA [4] Chapter 57 |
| 3.2. | The design approach proposed in this Safety Guide for the protection of items important to safety and, as applicable, of plant personnel performing actions to protect against internal hazards, is based on the following major steps:  (a) Identification of internal hazards and credible combinations of hazards, and characterization of the effects of the hazard(s);  (b) Design for preventing internal hazards or for preventing the adverse effects of internal hazards;  (c) Design of means for mitigating the adverse effects of internal hazards on items important to safety.  The design approach also includes the assessment of the protection against internal hazards, consistent with the design objectives in para. 2.12, and the verification that these objectives are met for all credible hazards at the plant. | NR | This is a statement not a requirement. |
| 3.3. | The design for the protection against internal hazards should take into account design recommendations for safety and design recommendations for security in an integrated manner, such that safety measures and security measures do not compromise each other. Recommendations on nuclear security are provided in Ref. [3]. | COM | The AP1000 plant safety and security measures have been developed in an integrated manner with active participation by utility organizations with plant operating experience. |
| 3.4. | Certain postulated internal hazards might be of such magnitude that providing design features to mitigate the effects of these hazards is not practicable (e.g. an uncontrolled drop of the reactor vessel head). In such cases, the focus is on prevention, and an evaluation should be performed to ensure, with a high level of confidence, that such events are extremely unlikely. Even if such events cannot be completely prevented, design measures are still required to be implemented to mitigate the consequences of such events to the extent practicable: see para. 2.8 of SSR‑2/1 (Rev. 1) [1]. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  To achieve the highest level of safety that can reasonably be achieved, the AP1000 plant design has been developed to provide such measures:   * 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. * 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 19 provides the PRA showing the extremely low likelihood of serious radiological consequences and that mitigation measures are effective for severe accidents. |
| 3.5. | In order to protect items important to safety, a nuclear power plant should have a sustained capability for the early detection and effective control of internal hazards. | COM | The AP1000 plant PRA [4], as summarized in the AP1000 plant DCD [2] Chapter 19, provides a systematic evaluation of events and failures. Safety-related SSCs are designed to continue to perform their safety functions in the event of an internal hazard as described in DCD [2] Chapter 3. |
| **IDENTIFICATION AND CHARACTERIZATION OF INTERNAL HAZARDS AND HAZARD COMBINATIONS** | | | |
| 3.6. | In plant design, internal hazards should be identified using a combination of engineering judgement, operating experience and lessons from similar plant designs, and the results of deterministic safety assessments and probabilistic safety assessments. The identification and the characterization of internal hazards should include a consideration of the initial conditions (e.g. plant shutdown modes), the magnitude and the likelihood of the hazards, the locations of the sources of the hazards, the resulting environmental conditions and the possible impacts on SSCs important to safety or on other SSCs for which failure could lead to a postulated initiating event. The hazard identification and characterization process should be rigorous, well documented and supported by plant walkdowns for verification purposes. | COM  OR  POS | The AP1000 plant design considers internal hazards as described in response to Section/Paragraph 3.1. Analyses for internal hazards have been performed deterministically as described in DCD [2] Chapter 2, DCD Chapter 3, DCD Appendix 9A, and probabilistically as described in DCD Chapter 19.  The site-specific identification of hazards is described in DCD Chapter 2. Identification of site-specific hazards is the responsibility of the Owner. |
| 3.7. | Possible combinations of internal–internal and internal–external hazards and any consequential effects (e.g. high energy pipe break, pipe whip, jet effect, flooding) are required to be considered in the design of the plant: see para. 5.32 of SSR‑2/1 (Rev. 1) [1]. The combinations to be considered will depend on the site characteristics and the general plant design.3  **\_\_\_\_\_\_\_\_\_\_**  3 For example, some combinations of hazards might involve external events that are not plausible in certain locations (e.g. sandstorms, blizzards). Therefore, it is not necessary or even feasible to prescribe a set of combined hazards that would be applicable to all sites. | COM  POS | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  The AP1000 plant PRA [4], 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 [9][10][11]. |
| 3.8. | All credible combination of hazards should be considered in the design. The screening out of any combinations should be justified (see Appendix I). | COM | All credible combination of hazards has been considered in the design. See responses to Section/Paragraph 3.7 and Appendix I. |
| 3.9. | The identification of hazards includes assumptions about their characteristics. Bounding or conservative assumptions could be made about these characteristics in order to address uncertainties, provided these assumptions are justified. | NR | This is a statement not a requirement. |
| 3.10. | Paragraph 5.15A of SSR‑2/1 (Rev. 1) [1] states:  “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 relevant internal hazards are required to be identified, and the effects and environmental conditions created by these hazards are required to be evaluated and taken into account in the design and layout of the plant: see Requirement 17 of SSR‑2/1 (Rev. 1) [1]. This is considered in paras 3.11–3.34, which also apply, as appropriate, to internal hazards resulting from combinations of hazards. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  The AP1000 plant design includes redundancy and physical separation of components as necessary to fulfill the plant’s safety functions. See response for compliance to US NRC GDCs 5, 13, 22, 24, 26 [8].  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). |
| **PREVENTION OF INTERNAL HAZARDS AND OF THE EFFECTS OF THE HAZARDS** | | | |
| 3.11. | Some hazards may be screened out either because they are physically impossible (e.g. heavy load drop if there is no lifting equipment) or by a stringent justification, including, at a minimum, very high quality design, manufacturing, construction, in‑service inspection and due consideration of feedback from operating experience. | NR | This is a statement not a requirement. |
| 3.12. | When hazards cannot be screened out, measures, including administrative ones, should be implemented to reduce the frequency and potential magnitude of the hazards and their effects on SSCs important to safety. This should be mainly achieved by reducing, as far as practicable, the potential sources of hazards (e.g. limiting the use of combustible materials and the presence of ignition sources), supported by surveillance and in‑service inspections. It can also be achieved by location and layout (e.g. ensuring the best orientation of fast rotating machines). | OR | Recommendations for preoperational, startup, and surveillance procedures will be provided by Westinghouse. However, the implementation of an administrative measures shall be the responsibility of the Owner. |
| **MITIGATION OF THE EFFECTS OF INTERNAL HAZARDS** | | | |
| 3.13. | For each internal hazard that is considered in the design, measures should be implemented to control and to limit the consequences. These measures will depend on the type of hazard and on the specific technical solutions included in the design. In general, specific measures for the detection of the occurrence of the respective hazard should also be included. | COM | 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, as demonstrated by the design PRA [4] and summarized in DCD Chapter 19. 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 results of the safety analyses as detailed in the AP1000 plant DCD [2] Chapter 6, Section 9.1, and Chapter 15 and the PRA [4] 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. |
| 3.14. | The design features for protection from the effects of internal hazards are required to be safety classified: see Requirement 22 of SSR‑2/1 (Rev. 1) [1]. This safety classification should be conducted in accordance with the recommendations provided in IAEA Safety Standards Series No. SSG‑30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants [4]. Protective design features are required to be classified on the basis of their function and their safety significance: see para. 5.34 of SSR‑2/1 (Rev. 1) [1]. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  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 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 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 APP-GW-G0R-005 [12]. |
| 3.15. | Measures to mitigate the consequences of events can be passive, active or procedural. Passive design solutions — without moving parts or an external energy supply — are generally considered preferable to the implementation of active measures or of procedures. | NR | This is a statement not a requirement. |
| 3.16. | For active protective features, where applicable, the worst single failure should be assumed. | COM | Failure of active components has been considered in the AP1000 plant design. The PRA [4] evaluates multiple failure events. 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 [4] 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. |
| 3.17. | The consideration of failure of a passive protective feature is not necessary, provided that it is demonstrated that its failure is very unlikely and that its function would remain unaffected by the postulated hazard (see para. 5.40 of SSR‑2/1 (Rev. 1) [1]). | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  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. |
| 3.18. | If it is feasible, the early detection of the occurrence of internal hazards, supported by appropriate actions in response to the detection of the hazard, contributes to the mitigation of the possible consequences. | NR | This is a statement not a requirement. |
| 3.19. | Measures for mitigation of the effects of internal hazards should include, as appropriate, redundancy, diversity and physical separation, including segregation of redundant trains. The concept of segregation is applicable at the following levels:  (a) Plant layout: for example, separating the emergency diesel generators from one another.  (b) Building layout: for example, mitigating the effects of missile hazards by proper orientation of equipment.  (c) Rooms and compartments: for example, dividing them into fire compartments or cells.  (d) SSCs: for example, separating cables of different safety trains from one another. | COM | The AP1000 plant design includes redundancy and physical separation of components as necessary to fulfill the plant’s safety functions. See response for compliance to US NRC GDCs 5, 13, 22, 24, 26 [8]. Also see the response for Paragraph 2.13 in APP-GW-GL-059 [7] where diversity between the DiD and the safety systems is discussed. |
| 3.20. | The layout and design provisions that protect SSCs important to safety from the effects of internal hazards should be such that the design objectives in para. 2.12 are met. | COM | See response to the Section/Paragraph 2.12. |
| 3.21. | The reliability of the means of detecting internal hazards and mitigating their consequences should be consistent with their role in providing defence in depth. | COM | 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. |
| **ASSESSMENT, VERIFICATION AND SUCCESS CRITERIA** | | | |
| 3.22. | To evaluate the adequacy of the design, qualitative and/or quantitative success criteria should be defined, consistent with the design objectives in para. 2.12. | COM | See response to Section/Paragraph 2.12. |
| 3.23. | An assessment should be made to demonstrate that the internal hazards relevant to the design of the nuclear power plant have been considered, and that provisions for prevention and mitigation have been designed with sufficient safety margins to address the uncertainties in the identification and characterization of internal hazards and their effects, as well as for the avoidance of cliff edge effects. This assessment should be carried out early in the design stage and should be documented. It should be updated before initial loading of the reactor with nuclear fuel, and kept up to date during plant operation. | COM  OR | Analyses for internal hazards have been performed deterministically as described in DCD Chapter 2, DCD Chapter 3, DCD Appendix 9A, and probabilistically as described in DCD Chapter 19. See responses to Sections/Paragraphs 3.1 and 3.7.  The Owner shall be responsible for ensure that the assessment will be updated before initial loading of the reactor with nuclear fuel, and during plant operation. |
| 3.24. | It should be a goal of the design that a single internal hazard does not trigger an accident, unless the hazard can be considered by itself as a postulated accident (e.g. pipe rupture). In particular, the design should ensure with a high level of confidence that a single internal hazard does not result in design extension conditions with core melting. If this cannot be achieved, the designer should demonstrate that the boundary conditions used in the analysis of the corresponding accident are not affected by the loads resulting from the internal hazard. | COM | 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, as demonstrated by the design PRA [4] and summarized in DCD [2] Chapter 19. 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. |
| 3.25. | The design features protecting the SSCs that are intended to be used under design extension conditions should be designed or verified for the loads, conditions and durations associated with these scenarios (e.g. effects of hydrogen combustion). These design features should be protected against the consequences of an internal hazard that occurs before design extension conditions have been completely mitigated. Best estimate design loads, conditions and durations can be used for the design or the verification of these protective features. | COM | Safety-related SSCs are designed to continue to perform their safety functions in the event of an internal hazard as described in DCD [2] Chapter 3. Systems containing safety-related equipment that function to mitigate DBAs have component redundancy so that their functions can be performed, even in the unlikely event of the most limiting single failure occurring coincident with the postulated DBA. |
| 3.26. | Deterministic safety analyses, supplemented if applicable by probabilistic analyses, should be performed to demonstrate the adequacy of the design of the protection against internal hazards. The design should be an iterative process accounting for the results of such safety analyses. | COM | Analyses for internal hazards have been performed deterministically as described in DCD [2] Chapter 2, DCD Chapter 3, DCD Appendix 9A, and probabilistically as described in DCD Chapter 19. |
| 3.27. | Internal hazards considered in the deterministic safety analyses for a specified location in the nuclear power plant include the following categories:  (a) Internal hazards that do not trigger, or result from, an anticipated operational occurrence or an accident;  (b) Internal hazards that could trigger, or result from, an anticipated operational occurrence;  (c) Internal hazards that could trigger, or result from, a design basis accident;  (d) Internal hazards that could trigger, or result from, design extension conditions without significant fuel degradation;  (e) Internal hazards that could result from design extension conditions with core melting. | NR | This is a statement not a requirement. |
| 3.28. | For internal hazards that do not trigger, or result from, an anticipated operational occurrence or an accident, an assessment should be performed to demonstrate that the plant can be brought to, and maintained in, a safe state even in the event of a single failure, including when equipment is unavailable owing to preventive maintenance considered in the design. In practice, a functional analysis is normally performed to demonstrate that an adequate number of functions remain available to reach and maintain a safe state. | COM | The AP1000 plant DCD [2] as a whole provides a comprehensive safety assessment. (See AP1000 plant DCD [2] Appendix 1B, Chapters: 15, 17, 19). All normal modes of operation are considered. In particular, the initiating event arising from an internal hazard is pessimistically assumed to occur simultaneously with the most adverse normal plant operating state or configuration (e.g. equipment outages for maintenance, test or repair). In addition, single failures in the safety measures are assumed in accordance with the single failure criterion. See also responses to Sections/Paragraphs 3.29, 3.30 and 3.31. |
| 3.29. | For internal hazards that could trigger, or result from, an anticipated operational occurrence, an assessment should be performed to demonstrate that the plant can be brought to, and maintained in, a safe state even in the event of a single failure, including when equipment is unavailable owing to preventive maintenance considered in the design. A specific analysis of transients is normally not necessary as this is provided by the corresponding analysis of anticipated operational occurrences. In such cases, the analysis of the internal hazards is limited to a functional analysis that should demonstrate that an adequate number of functions to control anticipated operational occurrences and to reach and maintain a safe state are provided by the design. | COM | The AP1000 plant safety systems are designed to mitigate DBAs with a single failure, as defined in the AP1000 plant DCD [2] Chapter 15. 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.  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. |
| 3.30. | For internal hazards resulting from accidents without significant fuel degradation, the objective of the assessment should be to demonstrate that the boundary conditions, in particular for systems credited in the accident analysis, are not affected by the hazard. A specific accident analysis is normally not necessary as this is provided by the corresponding accident analysis in which the rules for design basis accidents or the rules for design extension conditions without significant fuel degradation should be applied, as appropriate (see IAEA Safety Standards Series No. SSG‑2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants [5]). As stated in para. 2.11, design basis accidents or design extension conditions induced by internal hazards should be avoided to the extent practicable. If an internal hazard could lead to an accident without significant fuel degradation, the objective of the assessment should be to demonstrate that the fundamental safety functions are fulfilled and that the plant can be brought to, and maintained in, a safe state. | COM | 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. |
| 3.31. | For the deterministic assessment of an internal hazard triggered by design extension conditions with core melting, it should be demonstrated by using the corresponding rules [5] that the boundary conditions, in particular for systems credited in the accident analysis, are not affected by the hazard. It should be demonstrated that the SSCs necessary to maintain the integrity of the containment are not affected by the hazard. In particular, the integrity of instrumentation providing necessary measurements should be ensured. | COM | 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)).  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.  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. |
| **SPECIFIC ASPECTS OF DESIGN FOR PROTECTION AGAINST INTERNAL HAZARDS** | | | |
| 3.32. | For a site containing multiple units, steps should be taken to ensure that an internal hazard in one unit under construction, in operation or under decommissioning would not have any safety consequences for a neighbouring operating unit or other installations on the site (e.g. spent fuel pool, radioactive waste management facility). Measures for temporary separation should be put in place if necessary to protect the operating units. Consideration should be given to the possibility of internal hazards involving facilities shared between units: see para. 5.63 of SSR‑2/1 (Rev. 1) [1]. | POS | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  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. There is no sharing of safety systems between multiple units on a single site. |
| 3.33. | The main control room and the supplementary control room should be adequately separated from possible sources of internal hazards as far as applicable. The means by which the control is transferred from the main control room to the supplementary control room should be resilient against internal hazards to prevent malfunction or spurious actuation4.  **\_\_\_\_\_\_\_\_\_\_**  4 Spurious actuation of plant components (of the same type or combinations of different types of component) has the potential to place a given plant into an unsafe operating condition that might not be bounded by the plant’s safety analyses. | COM | The MCR is located in the non-radiologically controlled portion of the auxiliary building. The MCR is protected against the effects of both internal and external hazards. The MCR is designed, located, and protected such that a design basis radiological event in the plant cannot simultaneously affect key safety functions such as core cooling or spent fuel cooling and the operations of the MCR.  The MCR is a continuously occupied space designed to support and protect the operators. The MCR is equipped with fire detection and mitigation features, including application of linear heat detection in Class 1E cable tray, underfloor fire detection, accessibility for manual fire suppression actions, means of egress and accessibility of the remote shutdown room (RSR).  The effects upon habitability of the main control room resulting from postulated pipe breaks and cracks in the auxiliary building has been evaluated. See DCD [2] Section 3.6.1.2.2. Workstations and other equipment in the main control room are separated from piping (DCD [2] Section 3.7.3.13.1). SSCs whose failure results in incapacitating injury to the occupants of the main control room are classified as seismic Category II. See DCD [2] Section 3.2.1.1.2.  Seismic Category I equipment in the MCR includes the dedicated safety panel, VBS HVAC dampers, VES isolation valves, lighting circuits, and mounting for lighting fixtures. See DCD [2] Table 3.7.3-1.  With respect to fire protection, features are included in the main control room, as described in DCD [2] Section 1.9.5.1.6:   * Reduce the probability of fire initiation * Reduce the likelihood of fire spreading * Increase the probability of fire detections * Effectively mitigate the effects of a fire * Noncombustible and fire-resistant materials are used in the main control room   Additionally, the probability of fire within the MCR has been minimized by reducing the amount of the leading combustible loads via the reduction in the amount and type of cabling. The I&C design employs a digital control philosophy that utilizes fiber optic cabling and minimizes the use of current-carrying conductors, which is in contrast to traditional MCR designs. As a result, the overall amount of cabling, the amount of energized cable, and the risk of a fire are significantly reduced.  The main control room is shielded by the containment and auxiliary building from direct gamma radiation and inhalation doses resulting from the postulated release of fission products inside containment.  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 particulate or iodine radioactivity is detected in the MCR supply air duct, which would lead to exceeding US NRC GDC 19 [8] operator dose limits, the PMS automatically isolates the MCR, and operator habitability requirements are then met by the main control room emergency habitability system (VES). The main control room VES is capable of providing emergency ventilation and pressurization for the MCR. See DCD [2] Section 6.4.  The safety power sources and passive cooling capability in the MCR 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. After 3 days, it is possible to continue operation with the control room cooled and ventilated with circulation of outside air. In the event that the operators are forced to abandon the MCR, a remote shutdown workstation is provided with remote shutdown capability. A mechanism is provided to allow the operating staff to transfer control from the MCR to the remote shutdown workstation. The remote shutdown workstation is described in the AP1000 plant DCD [2] Section 7.4. |
| 3.34. | Additional guidance on assessment and verification of specific internal hazards is given in Section 4. Further information on the approach to hazard combinations is provided in Appendix I. | NR | This is a statement not a requirement. |

## 

## RECOMMENDATIONS FOR SPECIFIC INTERNAL HAZARDS

| **Section/Paragraph** | **Requirement**  **Note:** The references noted in [] in column “Requirement” do not relate to the reference list in Sections 4.0 of this document but relate to the reference list of the IAEA Specific Safety Guide SSG-64. | **Compliance** | **Justification** |
| --- | --- | --- | --- |
| **INTERNAL FIRES** | | | |
| **GENERAL** | | | |
| 4.1. | Nuclear power plants contain a range of combustible materials, as part of the structure, equipment, fluids, cabling or miscellaneous items in storage. Fire can be assumed to occur in any plant area where combustible materials are present. Where it is not practicable to eliminate these materials, design measures for fire prevention should be applied to all the fixed and transient (temporary) fire loads. Such measures include minimization of fixed fire loads, prevention of their accumulation, and control or (preferably) elimination of sources of ignition. | COM  OR | Westinghouse takes care to provide fire protection throughout the plant area. Fire hazard analysis considers the provision of fire control in AP1000 plant areas, with particular focus on those areas containing safety-related SSCs i.e. the NI buildings. Ignition sources are controllable through good plant design and implementation of operational procedures but cannot reliably be eliminated.  See DCD [2] Section 9.5 and Appendix 9A.  The Owner shall be responsible for providing control over the transient fire loads. |
| 4.2. | The design of fire prevention measures should start in the early stages of the design process. All such measures should be fully implemented before nuclear fuel arrives on the site. | COM  OR | Westinghouse provides consideration of fire prevention measures in the early stages of the design process. AP1000 fire prevention, control, detection, and suppression features provide plant and personnel safety. The fire protection analysis evaluates the adequacy of fire protection for systems and plant areas important to the generation of electricity. See DCD [2] Appendix 9A.  The Owner shall be responsible for ensuring the fire protection program is available in time for receipt of fuel and ensuring that quality assurance is maintained throughout operation. |
| **IDENTIFICATION AND CHARACTERIZATION OF FIRE HAZARDS** | | | |
| 4.3. | A fire hazard analysis of a plant site should be undertaken to demonstrate the overall adequacy of fire protection measures. In particular, the fire hazard analysis should determine the necessary fire resistance rating of fire barriers and the necessary fire detection and extinguishing capabilities (see the detailed recommendations on fire hazard analysis in Appendix II). | COM | The AP1000 fire protection analysis evaluates the potential for occurrence of fires within the plant and documents the capabilities of the fire protection system and the capability to safely shut down the plant. The fire protection analysis is an integral part of the process of selecting fire prevention, detection, and suppression methods, and provides a design basis for the fire protection system.  The purpose of the fire protection analysis is as follows:   * Identify the potential for fires based on the type, quantity, and location of combustible materials, * Determine the consequences of postulated fires, * Provide a basis for decisions on how to prevent, detect, contain, and suppress fires, * Assess fire protection system adequacy, * Confirm the capability to safely shut down the plant following a fire.   See Appendix 9A to the AP1000 plant DCD [2]. |
| 4.4. | The fire hazard analysis should be carried out in accordance with the recommendations in para. 3.23. | COM | The fire hazard analysis presented in the AP1000 plant DCD [2] was carried out in accordance with the recommendations in para. 3.23. |
| **FIRE PREVENTION** | | | |
| 4.5. | The following measures should be taken in the design to minimize the likelihood of internal fires:  (a) Removal, minimization and segregation of fixed and transient fire loads, as far as practicable.  (b) Elimination of potential ignition sources to the extent practicable; otherwise, the strict control of any such sources.  (c) Segregation of ignition sources from fuel sources. | COM | Fire prevention and control features are identified in the AP1000 plant DCD [2] Section 9.5.1.2.1.1. See also response to Section/Paragraph 4.1. |
| **MINIMIZING FIRE LOADS** | | | |
| 4.6. | Paragraph 6.54 of SSR‑2/1 (Rev. 1) [1] states that:  “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.” | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  Fire prevention and control features are identified in the AP1000 plant DCD [2] Section 9.5.1.2.1.1. |
| 4.7. | In order to reduce the fire load to the extent possible, thus minimizing the fire hazard, the following aspects should be considered in the plant design:  (a) The use of non‑combustible construction materials (e.g. structural materials, insulation, cladding, coatings, floor materials) and plant fixtures, as far as practicable.  (b) The use of non‑combustible air filters and filter frames, as far as practicable; otherwise low combustible materials could be used.  (c) The use of a protected pipe or double pipe design for lubricating oil lines and for collection of leakages.  (d) The use of hydraulic control fluids of low flammability for the control systems of steam turbines and other equipment.  (e) The selection of dry type transformers, as far as practicable.  (f) The use of non‑combustible materials in electrical equipment, such as switches and circuit breakers, and in control and instrumentation cubicles, and use of flame retardant non‑corrosive cables or cables with suitable qualifications.  (g) The use of non‑combustible scaffolding and staging materials.  (h) Segregation and compartmentation of fire loads, as far as practicable, to reduce the likelihood of fire and other effects spreading to other SSCs important to safety. | COM  OR | a) The plant is constructed of noncombustible materials to the extent practicable. The selection of construction materials and the control of combustible materials are in accordance with BTP CMEB 9.5-1 [5] and Section 3.3 of NFPA 804 [13] as specified in WCAP-15871, “AP1000 Assessment Against NFPA 804,” [14].  b) DCD [2] Section 9.4 describes the design of AP1000 plant ventilation systems. A manual deluge system exists for areas with combustible air filters if determined to be necessary by the fire protection analysis.  c) Leakage control has been considered.  d) DCD [2] Table 3.2‐3 includes principal construction codes for mechanical and fluid system components.  e) The AP1000 plant design does not have any indoor oil-filled transformers. Outdoor oil-filled transformers are located at least 50 ft (15 m) from the buildings or building walls within 50 ft (15 m) of oil filled transformers are without openings and have a 3-hour fire resistance rating.  f) Selection, application, and installation of onsite electrical equipment used in the AP1000 plant is guided by the design criteria, NRC Regulatory Guides, and IEEE Standards discussed in DCD [2] Section 8.1.4.2. See also DCD [2] Section 9.5.1.2.1.1. The insulating and jacketing material for electrical cables is selected to meet the fire and flame test requirements of IEEE Standard 1202 [15] or IEEE Standard 383 [16], excluding the option to use flame source, oil, or burlap.  g) This requirement shall be the responsibility of the Owner and/or Constructor. Other requirements of fire protection during construction are in accordance with BTP CMEB 9.5-1 [5] and Chapter 9 of NFPA 804 [13], as specified in WCAP-15871 [14].  h) In general, systems important to safety are located outside areas with high fire loads. Many of the systems important to safety are located inside containment, which is a light hazard fire area. Concentrations of combustible materials are located outside structures containing safety-related components. Where this is not possible, appropriate fire protection is provided. |
| 4.8. | Precautions should be taken to prevent thermal insulating materials from absorbing flammable liquids (e.g. oil). Suitable protective coverings or drip guards should be provided. | COM | The AP1000 plant design uses fire-retardant and heat-resistant materials, where practical, consistent with applicable industry guides, standards, and criteria. The plant is constructed of noncombustible materials to the extent practicable. The selection of construction materials and the control of combustible materials are in accordance with BTP CMEB 9.5-1 [5] and Section 3.3 of NFPA 804 [13], as specified in WCAP-15871 [14]. |
| 4.9. | Design measures should be implemented to provide for the proper storage of transient combustible materials that arise during operation; either separated from items important to safety, or otherwise protected. | COM | Transient combustible materials are controllable through good plant design and implementation of operational procedures but cannot reliably be eliminated. See DCD [2] Section 9.5 and Appendix 9A.  Combustible loadings for each fire area/zone are provided in DCD [2] Table 9A-3. Where the presence of transient combustibles is anticipated, their presence is indicated by the listing of volatiles or trash. See also response to Section/Paragraph 4.10. |
| 4.10. | Storage allowances for flammable liquids and gases inside plant buildings should be minimized. Storage areas for bulk supplies of any flammable or combustible materials should be located in areas or buildings that do not contain items important to safety. | COM  OR | Storage and control of flammable liquids, gases, and other materials are discussed in DCD [2] Section 9.5.1.2.1.1 and Table 9A-3. Initial locations of plant combustible materials are identified and evaluated in DCD [2] Appendix 9A. Storage areas are in areas or buildings that do not contain items important to safety.  Subsequent transporting, handling, storage, and relocation of combustible materials during the lifetime of the plant and their potential impact relative to proximity to safety items are the responsibility of the Owner. |
| 4.11. | Suitable fire rated storage cabinets should be provided to house any small quantities of flammable liquids or gases necessary to support plant operations. | OR | This requirement shall be the responsibility of the Owner. |
| 4.12. | Systems containing flammable liquids or gases should be designed to have a high degree of integrity in order to prevent leaks. They should be protected from degradation effects (e.g. corrosion) and destructive effects (e.g. vibration, effects of hazards) and maintained in good condition. Safety devices, such as flow limiting, excess flow and/or automatic shut‑off devices, and bunding and/or dyking devices, should be provided to limit potential spills in the event of a failure. | COM  OR  N/A | Hydrogen lines in safety-related areas are designed to Seismic Category I requirements. Storage of flammable liquids is intended to be in compliance with NFPA 30, “Flammable and Combustible Liquids Code” [13]. It is the responsibility of the Owner to ensure this compliance is maintained throughout the life of the plant.  A collection system is not necessary for the RCPs because the sealless motor RCPs used in the AP1000 plant design have no external lube oil system. The plant design includes dikes and curbs around oil tanks.  There is no drain path that could drain combustible liquids to the fire areas in the electrical portion of the nuclear island. For mechanical equipment fire areas in the nonradioactive auxiliary building, fires caused by potential transport of combustible liquid through the drain system are included in the fire hazards analysis.  The larger diesel fuel oil storage tanks are located in the yard, outside of the diesel generator building. They are located at least 50 ft (15 m) from any building containing safety-related equipment. Potential oil spills from the storage tanks are confined by a diked enclosure. The Owner shall be responsible for precaution regarding spillage of oil in the maintenance procedures.  The exterior and interior surfaces of the fuel oil storage tanks are painted with a primer and finish coat system for corrosion protection of the tank surface. Exterior surfaces of the diesel fuel oil transfer piping are painted for corrosion protection. Buried sections are enclosed in guard pipes to prevent leakage to the environment. The guard pipe containment system is corrosion resistant plastic, designed and fabricated for the site overburden wheel loads which result from equipment removal and replacement.  For further information see DCD [2] Section 9.3.2 (“Plant Gas System”), 9.5.4 (“Standby Diesel Fuel Oil System”) and Chapter 3 (“Design of Structures, Components, Equipment and Systems”). |
| **MINIMIZING IGNITION SOURCES** | | | |
| 4.13. | In the design, the number of ignition sources should be minimized to the extent practicable (e.g. a resilient design for the electrical protection system could be used). | COM | 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. See DCD [2] Section 9.5.1. |
| 4.14. | Systems that contain pressurized combustible liquids, such as hydraulic fluids and lubricating oil, should be provided with spray guards, as far as practicable. Equipment should be appropriately rated, consistent with the hazards present in the environment, to prevent it providing a source of ignition for flammable gases and ignitable sprays. | CWO | Systems that contain pressurized combustible liquids have been considered. Appropriate protective measures such as spray guards or drains are applied where necessary. |
| 4.15. | Potential ignition sources arising from plant systems and equipment should be controlled. | COM  OR  POS | Ignition sources are controlled as a defence-in-depth measure as far as reasonably practicable. These controls, relative to the specification of the AP1000 design, specify suitably rated equipment and management procedures to ensure such equipment undergoes adequate examination, maintenance, inspection, and testing (EMIT) to reduce the likelihood of a fault developing. Proper selection and maintenance of installed and portable equipment reduces the potential for creating accidental ignition sources. Evidence of such measures will be developed as part of the safety management procedures produced as part of the site-specific licensing.  The fire protection requirements during plant operation and maintenance are the responsibility of the Owner. |
| 4.16. | As far as is practicable, systems and equipment should be made safe through design, so as not to provide any ignition source. Where this is not practicable, such systems and equipment should be separated from combustible materials, or else insulated or enclosed. Equipment for dispensing flammable liquids or gases should be properly earthed. Hot pipework near combustible materials that cannot be moved elsewhere should be shielded and/or insulated. | COM | The AP1000 plant is designed to prevent fire initiation by controlling, separating, and limiting the quantities of combustibles and sources of ignition.  The grounding and lightning protection system (EGS) provides electrical grounding for instrumentation grounding, equipment grounding, and lightning protection during normal and off-normal conditions. The EGS provides an electrical grounding system for: equipment grounding of equipment enclosures, metal structures, metallic tanks, ground bus of switchgear assemblies, load centers, motor control centers, and control cabinets. Lightning protection is provided for exposed structures and buildings housing safety-related and fire protection equipment. See DCD [2] Section 2.6.6.  Hot pipework near combustible materials will be properly shielded and/or insulated. |
| 4.17. | Cables should be laid on trays or in installed conduits, or placed in other acceptable structures made out of non‑combustible materials; steel is often used for this purpose. The distances between power cables or cable trays should be sufficient to prevent the cables from heating up to unacceptably high temperatures. The electrical protection system should be designed so that the cables will not overheat under normal loads or transient short circuit conditions. Further recommendations are provided in IAEA Safety Standards Series No. SSG‑39, Design of Instrumentation and Control Systems for Nuclear Power Plants [6], and IAEA Safety Standards Series No. SSG‑34, Design of Electrical Power Systems for Nuclear Power Plants [7]. | COM | This requirement has been considered in the AP1000 plant design as described in DCD [2] Section 9.5.1.2.1.1. Moreover, the design, routing, and separation of cable and raceways are described in Section 8.3 of the AP1000 plant DCD [2]. |
| **FIRE MITIGATION** | | | |
| **TIMELY DETECTION AND EXTINGUISHING OF FIRES** | | | |
| 4.18. | Requirement 74 of SSR‑2/1 (Rev. 1) [1] states:  “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.”  These systems and equipment should be designed to provide a timely alarm in the event of fire, and the rapid extinguishing of fires, in order to minimize adverse effects on items important to safety and on plant personnel performing actions important to safety. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  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. * 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. * 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 (114 m3/h) 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. |
| 4.19. | Active and passive means of fire protection that are needed to protect SSCs important to safety against a fire following a different event (e.g. an earthquake) should be identified, adequately designed and qualified to resist the effects of this event. | COM | The fire protection system is classified as a nonsafety-related, nonseismic system. Special seismic design requirements are applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake, as described in DCD [2] Section 9.5.1.2.1.5. In addition, the containment isolation valves and associated piping for the fire protection system are safety-related and seismic Category I. The fire protection system is not required to remain functional following a plant accident or the most severe natural phenomena, except for a safe shutdown earthquake. See also DCD [2] Section 9.5.1.1.1. |
| 4.20. | Active and passive means of fire protection that do not need to maintain a functional capability following a postulated initiating event should be designed and qualified so that they do not fail in a way that could adversely affect safety. | COM | To achieve the required high degree of fire safety, and to satisfy fire protection objectives, the AP1000 plant is designed to provide confidence that failure or inadvertent operation of the fire protection system cannot prevent plant safety functions from being performed. DCD [2] Section 9.5.1 describes the fire protection system. |
| 4.21. | The need to minimize spurious alarms and discharges of extinguishing media should be taken into account in the design of fire detection and extinguishing systems and equipment. | COM | Fire protection system integrity has been considered in the AP1000 plant design. For fire areas containing safety-related components, the potential for a credible inadvertent actuation of automatic suppression systems is determined and the consequences are evaluated. See DCD [2] Section 9A.2.6. |
| 4.22. | Paragraph 6.51 of SSR‑2/1 (Rev. 1) [1] states:  “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.”  In addition, fire extinguishing systems should be designed and located so that they would not simultaneously affect redundant parts of safety groups, and thereby cause the measures taken to meet the single failure criterion to become ineffective. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  Automatic fire suppression systems are in accordance with Branch Technology Position (BTP) CMEB 9.5-1 [5] 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 DCD [2] Section 9.5.1. |
| 4.23. | Fire detection systems, fire extinguishing systems and support systems, such as ventilation and drainage systems, should, as far as practicable, be independent of their counterparts in other fire compartments. The purpose of this is to maintain the operability of such systems in adjacent fire compartments. | CWO | In general, fire areas containing redundant safety systems have a separate distribution header in accordance with DCD [2] Table 9A-4, but they are not completely separate ventilation systems in all cases. However, fire barrier penetration openings for ventilation are protected by fire dampers having a rating equivalent to that of the fire barrier. |
| 4.24. | The control of fire is achieved through a combination of fixed fire suppression and extinguishing systems and equipment and manual firefighting capabilities. To ensure an adequate level of protection for fire compartments, the following elements should be considered in the design of the plant:  (a) Where fire detection or extinguishing systems are credited as active elements of a fire compartment, arrangements for their design, procurement, installation, verification and periodic testing should be sufficiently stringent to ensure their permanent availability. In this case, the performance of these systems should be designed taking into account the application of the single failure criterion for the safety function they protect. The application of the single failure criterion is described in paras 5.39–5.40 of SSR‑2/1 (Rev. 1) [1].  (b) Where fire detection systems or fixed fire extinguishing systems are relied upon as protection against a potential fire following a different event (e.g. from external or internal hazards), they should be designed to withstand the effects of this event.  (c) The normal or the spurious operation of fire extinguishing systems should not impair the performance of safety functions. | CWO | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  a) Fire analysis follows the guidance of Branch Technical Position (BTP) CMEB 9.5-1 [5] to evaluate the consequence of fires within the plant, document the capabilities of the passive and active fire protection features and evaluate the impact of fire on the delivery of safety-related functions. None of the fire protection systems are required for safe shutdown. The design of automatic and manual suppression systems is reviewed to verify that there is no potential single impairment that incapacitates both the automatic suppression system and the manual suppression system, for fire areas where both types of suppression systems are provided. Areas without suppression or with only one type of suppression do not affect the ability to achieve safe shutdown, even if a single failure is assumed.  b) The fire protection system is classified as a nonsafety-related, nonseismic system. Special seismic design requirements are applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake, as described in DCD [2] Section 9.5.1.2.1.5.  c) 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 |
| 4.25. | The reliability of fire detection and extinguishing systems should be consistent with their role in providing defence in depth, and with the recommendations provided in SSG‑39 [6]. This also includes ensuring that water supplies (including mains supplies) and utility connections (fire hydrants) are maintained such that they will meet any necessary demand. | COM | The FPS provides a defense in depth functions and comprises of automatic fire detection, an alarm system, and firefighting equipment in order to:   * Detect fires early * Minimize fire spreading * Extinguish fires quickly |
| 4.26. | Each fire compartment should be equipped with suitable, effective and reliable fire detection and alarm features. | COM | The analysis for each fire area describes the fire area and associated fire zones, and identifies the principal systems and safety-related components in the fire area. Fire detection and suppression features are listed and the means of smoke control is discussed.  See DCD [2] Section 9A.2.1.  The installation of fire detectors is in accordance with NFPA 72 [13] and the manufacturer's recommendations. The selection and installation of fire detectors is also based on consideration of the type of hazard, combustible loading, the type of combustion products, and detector response characteristics. The types of detectors used in each fire area are identified in the fire protection analysis. |
| 4.27. | Paragraph 6.52 of SSR‑2/1 (Rev. 1) [1] states that:  “Fire detection systems shall be designed to provide operating personnel promptly with information on the location and spread of any fires that start.”  This information should be used when taking action to avoid adverse effects on SSCs important to safety. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  Fire detection and alarm systems are provided where required by the fire protection analysis, in accordance with BTP CMEB 9.5-1 [5] and NFPA 72 [13]. Fire detection and alarm systems are generally in accordance with NFPA 804 [13]. See DCD [2] Section 9.5.1. Refer to WCAP-15871 [14] for details. |
| 4.28. | When items such as fire pumps, water spray systems, ventilation equipment and fire dampers are controlled by fire detection systems, and where spurious operation would jeopardize safety functions, the operation of these items should be controlled by two diverse means of detection operating in series. The design should allow the operation of the system to be stopped if the actuation is found to be spurious. | COM | For fire areas containing safety-related components, the potential for a credible inadvertent actuation of automatic suppression systems is determined and the consequences are evaluated. The result is that inadvertent actuation of the FPS does not prevent plant safety functions from being performed. |
| 4.29. | Systems and equipment for fire suppression and fire extinguishing, including manual firefighting equipment, should be of sufficient capacity to ensure that later fires caused by re‑ignition (e.g. due to hot materials) are prevented. | COM | The AP1000 plant is designed to provide the capability to extinguish fires in any plant area, to protect site personnel, limit fire damage, and enhance safe shutdown capabilities. |
| **PREVENTING THE SPREAD OF FIRES** | | | |
| 4.30. | Early in the design stage, the plant buildings should be divided into fire compartments, as far as practicable, or, where that is not possible, into fire cells. | COM | The plant is subdivided into fire areas to isolate potential fires and minimize the risk of the spread of fire and the resultant consequential damage from corrosive gases, fire suppression agents, smoke, and radioactive contamination. Some fire areas are subdivided into fire zones to permit more precise identification of the type and locations of combustible materials, fire detection, and suppression systems. The subdivision into fire zones is based on the configuration of interior walls and floor slabs, and the location of major equipment within each fire area.  The fire protection analysis contains a description of plant fire areas, fire zones, fire barriers, and the protection of fire barrier openings, as well as a description of the separation between redundant safe shutdown components.  See DCD [2] Section 9.5.1.2.1.1 and Section 9A.2.7.1. |
| 4.31. | Building structures (including columns and beams) should have a suitable fire resistance rating. The fire stability rating (the mechanical load bearing capacity as well as the thermal load bearing capacity) of structural elements within a fire compartment, or that form the compartment boundaries, should not be less than the fire resistance rating of the fire compartment itself. | COM | Plant buildings use noncombustible structural materials, primarily reinforced concrete, gypsum, masonry block, structural steel, steel siding, and concrete/steel composite material. The selection of construction materials and the control of combustible materials are in accordance with BTP CMEB 9.5-1 [5] and Section 3.3 of NFPA 804 [13], as specified in WCAP-15871 [14].  Floors, walls and ceilings separating fire areas have a minimum fire rating of two hours and higher if determined necessary by analysis as shown in DCD Table 9A-3 [2]. Doors and dampers between fire areas have a rating of not less than 1 hour and higher if determined necessary by analysis.  Three-hour fire barriers are noncombustible and surround fire areas containing safety-related components.  Openings through fire barriers for pipe, conduit, and cable trays that separate fire areas are sealed or closed to provide a fire resistance rating equal to that required of the barrier.  Door openings in fire barriers are protected with equivalently rated doors, frames, and hardware. Fire doors are self-closing or provided with closing mechanisms.  Penetration openings for ventilation systems are protected in accordance with NFPA 90A [13]. |
| 4.32. | The plant layout should be such that combustible materials (solids, liquids and gases) are not in proximity to items important to safety, as far as practicable. The design aim should be to segregate items important to safety from high fire loads and to segregate redundant safety systems from each other. The aim of this segregation is to reduce the risk of fires spreading, to minimize secondary effects and to prevent common cause failures. | COM | Concentrations of combustible materials are located outside structures containing safety-related components. Where this is not possible, appropriate fire protection is provided. In general, systems important to safety are located outside areas with high fire loads. Many of the systems important to safety are located inside containment, which is a light hazard fire area. The goal of fire protection for the AP1000 plant design is to separate redundant safe shutdown components and associated electrical divisions to preserve the capability to safely shut down the plant following a fire. |
| 4.33. | The segregation of redundant parts of a safety system ensures that a fire affecting one division5 of a safety system would not prevent the execution of the safety function within another division. This should be achieved by locating each redundant division of a safety system in its own fire compartment or at least in its own fire cell. The number of penetrations between fire compartments of different redundant divisions should be minimized and the penetrations should be sealed in a qualified manner.  **\_\_\_\_\_\_\_\_\_\_**  5 A system or set of components can be divided into redundant ‘divisions’ to allow for the implementation and maintenance of physical, electrical and functional independence with respect to other redundant sets of components [8]. | COM | Redundant safe shutdown components and associated electrical divisions are separated to preserve the capability to safely shut down the plant following a fire. Three-hour fire barriers provide complete separation of redundant safe shutdown components, including equipment, electrical cables, instrumentation and controls, except where the need for physical separation conflicts with other important requirements as identified in DCD [2] Section 9.5.1.2.1.1. |
| 4.34. | The effects of postulated fires should be analysed for all areas containing items important to safety and all other locations that constitute a fire hazard to items important to safety. In the analysis, the functional failure of all systems important to safety within the fire compartment or the fire cell in which the fire is postulated should be assumed, unless they are protected by qualified fire barriers or surrounded by casings, enclosures or encapsulations designed to (or able to) withstand the consequences of the fire. Exceptions should be justified. | COM | The effects of the postulated fires have been analyzed. A deterministic fire protection analysis is provided in DCD [2] Appendix 9A. In addition, a fire risk assessment was performed as discussed in Chapter 57 of the overall Probabilistic Risk Assessment (PRA) for the AP1000 plant. |
| **MITIGATION OF SECONDARY FIRE EFFECTS** | | | |
| **GENERAL** | | | |
| 4.35. | The hazardous (direct and indirect) effects of fire are the production of smoke (with the consequent possibility of its spreading to other areas not affected by the originating fire); radiative and convective heat; flame, which might lead to the further spread of fire, to equipment damage, to functional failures and to possible explosive effects; the production of other fire by‑products; as well as pressure buildup and reduction of oxygen levels. Effects due to fire extinguishing should also be considered. | COM | The hazardous effects of fire are considered in the  DCD [2] Section 9.5.1, Appendix 9A and in PRA [4]. |
| 4.36. | The main objectives in mitigating the effects of a fire are as follows:  (a) To confine the flame, heat and smoke in a limited space within the plant to minimize spread of the fire and consequent effects on the surrounding plant;  (b) To provide safe escape routes and access routes for personnel;  (c) To provide access for manual firefighting, manual actuation of fixed extinguishing systems and operation by plant personnel of systems necessary to reach and maintain safe shutdown;  (d) To provide the means for venting of smoke and heat either during or following a fire, if necessary;  (e) To control the spread of the extinguishing agents to prevent damage to items important to safety. | NR | This is a statement not a requirement. |
| **LAYOUT OF BUILDINGS** | | | |
| 4.37. | The layout of buildings, equipment, plant ventilation systems, and fixed fire detection and extinguishing means should all be taken into account in considering the mitigation of fire effects. | COM | These items have been taken into consideration. For further information see DCD [2] Chapter 9.5. See also responses to Sections/Paragraphs 4.18, 4.29 and 4.31. |
| 4.38. | Requirement 36 of SSR‑2/1 (Rev. 1) [1] states that:  “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.”  Adequate access routes for the firefighting teams or field plant personnel should also be provided and these should be protected. The use of combustible materials (e.g. lighting, paints, coatings) in escape routes and access routes should be limited, as far as practicable. The layout of buildings should be arranged to prevent the propagation of fire and smoke from adjacent fire compartments or fire cells to the escape routes or access routes. Further details are given in Appendix II. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  The AP1000 plant DCD [2] Section 1.2, Section 9.5.1, 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. See also response to Section/Paragraph II.22. |
| **VENTILATION SYSTEMS** | | | |
| 4.39. | Ventilation systems should neither compromise building compartmentation nor compromise the availability of redundant divisions of safety systems. These conditions should be addressed in the fire hazard analysis. | CWO | See response to Section/Paragraph 4.23. DCD [2] Section 9.4 describes design of the AP1000 plant ventilation systems. Appendix 9A to DCD [2] describes the Fire Protection Analysis. |
| 4.40. | Each fire compartment containing a redundant division of a safety system should have a ventilation system designed such that a fire in one safety fire compartment will not propagate fire effects that induce a loss of ventilation of another safety fire compartment. Parts of the ventilation system (e.g. connecting ducts, fan rooms) that are located in an adjacent fire compartment should have the same fire resistance rating as the compartment or, alternatively, the fire compartment penetration should be isolated by appropriately rated fire dampers. These should operate automatically, where appropriate. | COM | Fire compartmentation is used within the design of the AP1000 plant to ensure that an internal fire does not propagate. The number of penetrations in fire compartment barriers including ventilation ductwork, cables and pipework, is minimized as far as possible. Penetrations are fire stopped to the same fire resistance (integrity and insulation) as the barrier they penetrate; this reduces the potential routes for the spread of fire and hot gases. Fire dampers, and doors penetrating fire barriers are also fire rated for integrity and insulation from both sides will comply with the relevant parts of the appropriate standards. See also responses to Sections/Paragraphs 4.31 and 4.41. |
| 4.41. | If a ventilation system serves more than one fire compartment, provision should be made to maintain the segregation between fire compartments. Means should be provided to prevent the spread of fire, heat or smoke to other fire compartments by installing fire dampers at the boundaries of each fire compartment or by installing fire resistant ductwork, as appropriate. | COM | DCD [2] Section 9.5.1.2.1.1 describes plant fire protection and control features of the AP1000 plant. DCD [2] Section 9.4 describes the design of AP1000 plant ventilation systems.  Fire barrier penetration openings for ventilation are protected by fire dampers having a rating equivalent to that of the fire barrier.  Ventilation system fire dampers close automatically against full airflow on high temperature to control the spread of fire and combustion products. Fire dampers serving certain safety-related, smoke-sensitive areas are also closed in response to an initiation signal from the fire detection system. Smoke is removed from the fire area as described in the fire protection analysis. The fire protection analysis verifies that the ventilation system for the fire area does not contribute to the spread of fire or smoke. See Appendix 9A to the DCD [2]. |
| 4.42. | Charcoal filter banks contain a high fire load. These should be taken into consideration in determining recommendations for fire protection. A fire in a filter bank could lead to a radioactive release: consequently, passive and active means of protection should be provided to protect charcoal filter banks from fire. Such measures could include the following:  (a) Locating the filter in a fire compartment.  (b) Monitoring of the air temperature and automatic isolation of the air flow.  (c) Provision of automatic protection by means of a water sprinkler to cool the outside of the filter vessel.  (d) Provision of a suitable extinguishing system inside the filter vessel. In designing a water based extinguishing system for that purpose, consideration should be given to the flow rate of the water. If it is too low, the reaction between burning charcoal at high temperature and water can result in the production of hydrogen, which might induce another fire or explosion hazard. To prevent this risk, a high water flow rate should be used. The water injected into the filter housing should be drained or considered as an additional weight in the filter design. | COM | Charcoal filter banks have been considered in DCD [2] Appendix 9A and Chapter 9.5. Considerations include information e.g. about:   * The fire areas in which the filters are located, * The temperature limits of the filters, * The filters temperature monitoring system and fire detection system, * The classification regarding flammable materials, * The method of extinguishing filters. |
| 4.43. | Where combustible filters need to be used in ventilation systems or filtration units and the subsequent malfunction or failure of these filters could result in unacceptable radioactive releases, the following precautions should be taken:  (a) Filter banks should be separated from other equipment by means of adequate fire barriers.  (b) Appropriate means (e.g. upstream and downstream dampers) should be used to protect the filters from the effects of fire.  (c) Fire detectors, carbon monoxide gas sensors and/or temperature sensors should be appropriately installed to inform the plant personnel of a fire in the filter bank. | CWO | Charcoal beds are included in the fire protection analysis and appropriate fire barriers are applied according to this analysis (with one exception listed below).  Charcoal is contained within the following areas:   * 1242 AF 12401B MCR shift supervisor/clerk/operator areas – This area only contains approximately 99 lbs. (45 kg) of charcoal. * 1250 AF 01 VBS MCR/A&C equipment room uses a charcoal bed deluge – In the unlikely event of a fire in the adsorber, the filtration unit can be manually isolated. The adsorber bed deluge piping will be connected to a nearby hose station to cool the charcoal and extinguish the fire. * 4052 AF 40551 containment air filtration exhaust rooms A and B use a charcoal bed deluge – In the unlikely event of a fire in the adsorber, the filtration unit can be manually isolated. The adsorber bed deluge piping will be connected to a nearby hose station to cool the charcoal and extinguish the fire. * 1210 AF WGS delay bed room – There is charcoal in this room that is not mentioned in the standard plant fire protection analysis. A corrective action has been opened to ensure this is addressed in the next revision of the analysis.   A manual deluge system exists for areas with combustible air filters if determined to be necessary by the fire protection analysis. |
| 4.44. | The intakes for the fresh air supply to the fire compartments should be located at a distance from the exhaust air outlets and smoke vents of other fire compartments, to the extent necessary to prevent the intake of smoke or combustion products and the malfunction of items important to safety. | COM | Air intakes for ventilation systems are located remotely from the exhaust air outlets and smoke vents of other fire areas. |
| **FIRES AND POTENTIAL RADIOACTIVE RELEASES** | | | |
| 4.45. | Equipment that could release radioactive substances in the event of a fire should be identified in the fire hazard analysis. This equipment should be housed in separate fire compartments in which the designed fire loads, both fixed and transient, are minimized. | COM | As described in the fire protection analysis, materials that collect or contain radioactivity, such as spent ion exchange resins and filters, are protected and stored in accordance with BTP CMEB 9.5-1 [5]. See DCD [2] Section 9.5.1 and Appendix 9A. |
| 4.46. | The design should provide for heat and smoke venting in fire compartments containing radioactive materials. Although venting can result in a radioactive release to the external environment, it can prevent, directly or through the improvement of conditions for fire extinguishing, the subsequent release of larger quantities of radioactive substances. Two cases should be distinguished, as follows:  (a) The possible release can be shown to be well below regulatory limits.  (b) The amount of radioactive material in the fire compartment could produce a radioactive release exceeding the regulatory limits. In this case, provisions should be made for isolating the ventilation or closing fire dampers.  In each case, monitoring of the vented air should be performed to inform operational decision making. | COM | 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. Release of smoke and gases containing radioactive materials to the environment is monitored. The radiation monitoring for the ventilation systems is described in DCD [2] Section 9.4.  The AP1000 FPS is designed to minimize exposure to personnel and releases to the environment of radioactivity or hazardous chemicals as a result of a fire.  See also response to Section/Paragraph 4.47. |
| 4.47. | Design measures are required to be taken to keep the amount of radioactive material released as low as reasonably achievable: see Requirement 34 of SSR‑2/1 (Rev. 1) [1]. The design is required to include provisions for monitoring the condition of filters (see para. 6.63 of SSR‑2/1 (Rev. 1) [1]), in order to assist plant personnel in taking operational decisions. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  The AP1000 plant SSCs that provide radiation protection are described in 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.  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. * 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.   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.  See AP1000 plant DCD [2] Section 11.3.3. |
| **LAYOUT AND SYSTEMS FOR ELECTRICAL EQUIPMENT** | | | |
| 4.48. | Cabling for redundant safety systems should be installed in individual specially protected routes, preferably in separate fire compartments, as far as practicable, and cables should not cross between redundant divisions of safety systems. As described in para. II.17, exceptions may be necessary in certain locations, such as control rooms and the reactor containment. In such cases, the cables should be protected by means of qualified fire rated barriers or encapsulations (e.g. qualified cable wraps). Fire extinguishing systems or other appropriate means could be used, with justifications made in the fire hazard analysis. | COM | Redundant safety-related cable systems are separated from each other and from potential fire exposure hazards in non-safety-related areas by 3-hour rated fire barriers. There are five separation groups for the cable and raceway system: groups A, B, C, D, and N. Separation group A contains safety-related circuits from division A. Similarly, separation group B contains safety-related circuits from division B; group C from division C; group D from division D; and group N from non-safety-related circuits. Cables of one separation group are run in separate raceway and physically separated from cables of other separation groups.  Electric cable construction will pass the flame test in IEEE 1202 or IEEE 383 [15, 16], excluding the option to use the alternate flame source, oil or burlap.  Water based fire protection system is provided as the primary fire suppression for cable fires. The fire is extinguished manually using hose streams or portable extinguishers, except fire zone 11300B, which has a deluge system. All safety-related cable trays have line-type heat detectors.  See Appendix 9A to the AP1000 plant DCD [2]. |
| 4.49. | All possible fire induced failures that could affect redundant systems performing safety functions should be analysed (e.g. by electrical circuit analysis, including multiple spurious actuations). Electrical circuits should be rerouted or protected by combinations of qualified fire rated barriers and fire extinguishing systems, with appropriate justifications made in the fire hazard analysis. | COM | All openings for cable and cable tray penetrations are provided with penetration seals having a fire protection rating consistent with the designated fire resistance rating of the barrier. Penetration design complies with the guidelines of BTP CMEB 9.5-1 [5]. See also response to Section/Paragraph 4.48. |
| **SPECIAL LOCATIONS** | | | |
| 4.50. | The main control room of a nuclear power plant generally contains control equipment of different safety systems in close proximity. Particular care should be taken to ensure that, as far as practicable, non‑combustible materials are used in electrical cabinets, the room structure itself, any fixed furnishings, and floor and wall finishes. Redundant equipment used to perform the same safety function should be housed in separate electrical cabinets. Fire barriers should be utilized to the extent possible to provide any necessary separation. Every effort should be made to keep the fire load in control rooms to a minimum. | COM | Main Control Room description is contained within the following DCD [2] Sections:   * DCD Section 1.2.1.5.3 – Control Room Design * DCD Section 6.4.1.1 – Main Control Room Design Basis * DCD Section 7.1.1 – The AP1000 Instrumentation and Control Architecture * DCD Section 7.5 – Safety Related Display Information * DCD Section 18.8 – Human System Interface Design   Main control room fire area is described in Appendix 9A to the DCD [2] and in Section 9A.3.1.2.5.1 (“Fire Area 1242 AF 01”). Since the main control room is continuously manned, a fire is likely to be initially detected by an operator. Otherwise, a fire in this fire area is detected by a fire detector, which produces visual and audible alarms in the main control room and the security central alarm station. The fire is extinguished manually using portable extinguishers or, if necessary, using hose streams. Combustible materials in this fire area are listed in DCD [2] Table 9A-3, and primarily consist of cable insulation and paper.  Generally, three-hour fire barriers provide adequate separation from adjacent fire areas and the fire is contained within the fire area. Due to the need to provide passive cooling capability into the main control room ceilings, it will not be protected against fires from within the main control room. The ceiling will be a fire barrier from fires in the room above the main control room.  Three-hour fire barriers provide complete separation of redundant safe shutdown components, including equipment, electrical cables, instrumentation and controls, except where the need for physical separation conflicts with other important requirements, specifically:   * Fire barrier separation is not provided within the main control room fire area because functional requirements make such separation impractical. The risk of fires in the control room is minimized by the reduction in the quantity of electrical cables. Continuous occupancy provides confidence that fires would be quickly detected and suppressed. Should a fire require evacuation of the main control room, the plant can be safely shut down using independent controls at the remote shutdown workstation, located in a separate fire area. * Fire barrier separation is not provided between the main control room and the room above it from fires in the main control room. There are no safe shutdown components in the room above. There is fire barrier separation between the main control room and the room above it for fires in the room above. * Fire barrier separation is not provided within the remote shutdown room fire area because the remote shutdown workstation is not required for safe shutdown unless a fire requires evacuation of the main control room.   With respect to fire protection, features are included in the main control room, as described in DCD [2] Section 1.9.5.1.6 :   * Reduce the probability of fire initiation * Reduce the likelihood of fire spreading * Increase the probability of fire detections * Effectively mitigate the effects of a fire * Noncombustible and fire-resistant materials are used in the main control room. |
| 4.51. | In order to ensure their habitability, the main control room and the supplementary control room should be protected against the ingress of smoke and combustion gases and against other direct and indirect effects of fire and of the operation of extinguishing systems. | COM | Main control room habitability is described in DCD [2] Section 6.4. Protection measures of the main control room are described in DCD [2] Chapter 9 and Appendix 9A. |
| 4.52. | The fire protection of the supplementary control room should be similar to that of the main control room. Particular emphasis should be placed on protection from flooding and other effects of the operation of fire extinguishing systems. The supplementary control room should be located in a fire compartment separate from the one containing the main control room. The ventilation system for the supplementary control room should not be a common system shared with the main control room. The separations between the main control room and the supplementary control room should meet the design objectives in para. 2.12(e). | COM | Remote Shutdown Room description is contained within the following DCD [2] Sections:   * DCD Section 7.1.1 – The AP1000 Instrumentation and Control Architecture * DCD Section 7.4.3.1.1 – Remote Shutdown Room/Remote Shutdown Workstation * DCD Section 7.5 – Safety Related Display Information * DCD Section 18.8 – Human System Interface Design   The remote shutdown room is separated from other areas of the plant by 3-hour fire barriers. Portable fire extinguishers and hose stations are provided. A fire in this fire area is detected by a fire detector that produces an audible alarm locally; and both visual and audible alarms in the MCR and the security central alarm station. The outside air intake for the control room ventilation system is provided with smoke detection capability and enables the operator to isolate the remote shutdown room ventilation system and thus prevent smoke from entering the room. To the extent possible, all cables that enter the remote shutdown room terminate in the remote shutdown room. There are no underfloor spaces in the remote shutdown room that are used as distribution plenums. All cables are in covered cable trays or conduit. |
| 4.53. | The reactor containment is a fire compartment in which items of equipment for redundant divisions of safety systems might be close to each other. Redundant divisions of safety systems should be located as far apart as practicable and should be protected, where possible, by passive protection measures such as partial fire enclosures and cable fire protection systems. | COM | The containment is divided into fire zones, which are based on the establishment of boundaries (structures or distance) that inhibit fire propagation from zone to zone. Complete fire barrier separation cannot be provided inside containment because of the need to maintain the free exchange of gases for purposes such as passive containment cooling.  Fire detection is provided for safety-related cable trays inside containment. The quantity and arrangement of the combustible materials in the fire zones, and the characteristics of the barriers that separate one zone from other zones are such that a fire which damages safe shutdown components in one zone does not propagate to the extent that it damages redundant safe shutdown components in another fire zone. |
| 4.54. | Reactor coolant pump motors containing a large inventory of flammable lubricating oil should be provided with fire detection systems, fixed fire extinguishing systems (normally under manual control) and oil collection systems (e.g. oil pans). The oil collection systems should be capable of collecting oil and water from all potential leakage points or discharge points and draining these to a vented container or another safe location. | COM  N/A | The reactor coolant pumps (RCPs) are located in the steam generator compartments inside containment. The quantity of combustible materials in this fire zone is very low, consisting primarily of cable insulation related to the RCP motors and other components in this fire zone. The fire protection analysis includes a description of this fire area and its fire barriers, its associated fire zones, as well as fire detection and suppression capabilities.  See Appendix 9A for the DCD [2]:   * Section 9A.3.1.1 (“Containment/Shield Building”) * Section 9A.3.1.1.9 (“Fire Zone 1100 AF 11301”) * Section 9A.3.1.1.10 (“Fire Zone 1100 AF 11302”)   A collection system is not necessary for the RCPs because the sealless motor RCPs used in the AP1000 plant design have no external lube oil system. The plant design includes dikes and curbs around oil tanks. No automatic suppression systems are needed due to the sealless motor reactor coolant pumps (RCPs) having no external lube oil system.  See also DCD [2] Section 9.5.1.2.1.1. |
| 4.55. | Provisions similar to those described in para. 4.54 should be made for oil filled transformers, as applicable. | COM | Automatic deluge systems are provided. Outdoor oil-filled transformers have oil containment features or drainage away from the building. |
| 4.56. | The turbine building could contain items important to safety. Fire compartmentation might be difficult in some areas, and substantial fire loads are present such as large inventories of flammable materials in the lubricating, cooling and hydraulic systems of the steam turbine(s) and in the hydrogen atmosphere within the generator(s). Consequently, in addition to fire suppression systems, adequate oil collection systems (e.g. oil pans) should be provided for all equipment containing flammable liquids. The use of flammable hydrocarbon based lubricating fluids should be minimized. If flammable liquids have to be used, they should be liquids with high flashpoints, consistent with operational needs. | CWO | Systems that contain combustible liquids have been considered. Appropriate protective measures such as suppression systems or collection systems are applied where necessary. Protection measures have been provided in accordance with the Fire Protection Analysis. See Appendix 9A to the AP1000 plant DCD [2]. |
| 4.57. | The safety features for design extension conditions that are needed to function in the long term under such conditions should be protected against the effects of a fire. | CWO | The fire protection system is classified as a nonsafety-related, nonseismic system. Special seismic design requirements are applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake, as described in DCD [2] Section 9.5.1.2.1.5. |
| 4.58. | Equipment of the systems used for long term heat removal from the containment during severe accidents should be redundant or diverse and located in different fire compartments. | COM | A combination of redundancy and diversity has been provided for the equipment of the systems used for long term heat removal from the containment. |
| 4.59. | Ventilation equipment necessary in the long term during severe accidents to confine radioactive material should be redundant and located in different fire compartments. Portions of the system containing charcoal filters should be capable of being isolated and should be designed with suitable fire protection features (see para. 4.42). | COM | Radiologically controlled area ventilation system automatically isolates selected building areas from the outside environment by closing the supply and exhaust duct isolation dampers and starting the containment air filtration system when high airborne radioactivity in the exhaust air duct or high ambient pressure differential is detected. See DCD [2] Section 9.4.7 for a description of the containment air filtration system. See also responses to the Sections/Paragraphs 4.42 and 4.47. |
| **INTERNAL EXPLOSIONS** | | | |
| **GENERAL** | | | |
| 4.60. | Explosion hazards should be eliminated by design, as far as practicable. Priority should be given to design measures that prevent or limit the formation of explosive mixtures. | COM | The AP1000 plant design provides protection for internal hazards such as explosions. Explosions are addressed as described in DCD [2] Section 2.2 (Site-specific hazards, explosion by on-site storage facilities, flammable vapor clouds by on-site flammable liquids or gases) and DCD [2] Table 2.2.‐1 to establish safe distances with respect to on‐site explosions. See also DCD [2] Section 3.1.1, Criterion 3. |
| **IDENTIFICATION AND CHARACTERIZATION OF EXPLOSION HAZARDS** | | | |
| 4.61. | Explosion hazards within buildings and compartments containing items important to safety, and for other locations that constitute a significant explosion hazard to these areas, should be identified. Chemical explosions (typically explosions of gas mixtures), boiling liquid expanding vapour explosions induced by fire exposure, oil mist, blast from pressure vessel failure and high energy arcing faults6 accompanied by rapid air expansion and plasma buildup should be considered.  **\_\_\_\_\_\_\_\_\_\_**  6 High energy arcing faults are energetic or explosive electrical equipment faults characterized by a rapid release of energy in the form of heat, light, vaporized metal and pressure increase due to high current arcs between energized electrical conductors or between energized electrical components and neutral or ground. Such faults might also result in projectiles being ejected from the electrical component or cabinet of origin and result in fire. | COM | The AP1000 plant design considers internal explosions as described in DCD [2] Section 2.2 (Site-specific hazards, explosion by on-site storage facilities, flammable vapor clouds by on-site flammable liquids or gases). |
| 4.62. | Consequent effects of explosions (e.g. the rupture of pipes conveying flammable gases) should be taken into account in the identification of explosion hazards. | COM | The explosion effects have been considered in the AP1000 plant design. |
| **PREVENTION OF EXPLOSION HAZARDS** | | | |
| 4.63. | Flammable gases and liquids and combustible materials that could produce or contribute to explosive mixtures should be excluded from compartments (i.e. enclosed areas separated by barriers) that protect items important to safety against other internal hazards. Such flammable gases and liquids and combustible materials should also be excluded from areas adjacent to such compartments or areas connected to these compartments by ventilation systems. Wherever this is not practicable, quantities of such materials should be strictly limited and adequate storage facilities should be provided. Reactive substances, oxidizers and combustible materials should be segregated from each other. | COM | The quantity of potentially explosive material required for normal operating processes by the AP1000 design has been identified and storage facilities have been sized to minimize the severity of explosions that could occur. Safe distances for the storage facilities from the containment and auxiliary buildings have been determined, such that the maximum resulting explosive overpressures will not damage the structure and hence the SSCs protected by the structure. The AP1000 plant safe distance for material in onsite storage facilities for explosions, flammable vapor clouds, and fires is tabulated in DCD [2] Table 2.2-1. |
| 4.64. | Vessels containing compressed flammable gases should be securely stored in dedicated compounds that are located away from main plant buildings and provide appropriate protection from local environmental and hazardous conditions. | COM | The AP1000 plant safe distance for material in onsite storage facilities for explosions, flammable vapor clouds, and fires is tabulated in Table 2.2-1 in the DCD [2].  The nitrogen, the carbon dioxide, and the hydrogen system storage is located outside of the main buildings. The storage tanks are analyzed as a potential missile source. Refer to DCD [2] Section 3.5. Accidents involving accidental detonations of hydrogen from the onsite storage of compressed or liquid hydrogen are evaluated for damage to safety–related structures, systems, and components. Refer to DCD [2] Section 2.2. For explosions, the plant gas system is designed for conformance with Regulatory Guide 1.91.  The bulk gas storage area for the plant gas system (PGS) is located sufficiently far from the nuclear island that an explosion would not result in damage to safety-related structures, systems, and components.  Each storage vessel is hydrostatically tested in accordance with the ASME Boiler and Pressure Vessel Code, Section VIII, Division 1, 1998. Moreover, each vessel is examined using the magnetic particle method. See also DCD [2] Chapter 9. |
| 4.65. | In order to prevent a fire induced explosion from affecting items important to safety, consideration should be given to the provision of automatic systems for the detection of flammable gas releases, for isolation of the gas supply, if possible, and for fire extinguishing. | COM | The safety-related structures, systems, and components are designed to minimize the probability and effect of fires and explosions.  Equipment and facilities for fire protection, including detecting, alarming, and extinguishing functions, are provided to help protect both plant equipment and personnel from fire, explosion, and the resultant release of toxic vapors. Fire protection is provided by deluge systems (water spray), sprinklers, and portable extinguishers. |
| 4.66. | Hydrogen supply vessels and their distribution manifolds should be placed in well ventilated external locations that are separated from plant areas containing items important to safety. If such equipment has to be placed indoors, it should be positioned in a location that is remote from areas containing items important to safety. Interior storage locations should be provided with a ventilation system designed to ensure that the hydrogen concentration is kept at a safe level below the lower flammability limit in the event of a leak of gas. Hydrogen detection equipment should be provided and should be designed to give an alarm at a suitably low gas concentration. | COM | Gaseous hydrogen is supplied to the nuclear island from bottles (high-pressure tanks) adjacent to the turbine building and near the nuclear island. The hydrogen supply is not located in an indoor compartment that contains safety-related systems or components. The quantity that could be released in the event of a failure of the hydrogen supply would not lead to an explosion even if the full contents of the connected storage is assumed to remain in the compartment in which it is released. Mixing within a compartment is achieved by natural convection caused by thermal forces from hot surfaces and air movement due to operation of HVAC systems. The hydrogen supply line is not routed through compartments that do not have air movement due to HVAC systems.  The bulk gas plant storage area for the plant gas system (PGS) stores liquid hydrogen for use in generator cooling. The liquid hydrogen is converted to gas in the storage area and then piped to the generator in the turbine building. The turbine building includes sufficient ventilation to prevent an explosive concentration of hydrogen in the event of a leak.  The plant gas system is designed in accordance with the provision of onsite explosive materials addressed in NRC Regulatory Guide 1.91, “Evaluation of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plant Sites” [17]. |
| 4.67. | Where turbogenerators are cooled using hydrogen, monitoring equipment should be provided to indicate the pressure and purity of the hydrogen within the cooling system. Provision should be made to purge hydrogen filled components and related systems of pipes and ducts with an inert gas such as carbon dioxide or nitrogen before filling or when draining. | COM | The hydrogen gas portion of the plant gas system supplies hydrogen to the main plant electrical generator for cooling as well as to other plant auxiliary systems. Generator supervisory instruments are provided in AP1000 plant, with sensors and/or transmitters mounted on the associated equipment. These indicate or record the following:   * Multiple generator stator winding temperatures; the detectors are built into the generator, protected from the cooling medium, and distributed around the circumference in positions having the highest expected temperature * Stator coil cooling water temperature (one detector per coil) * Hydrogen cooler inlet gas temperature (two detectors at each point) * Hydrogen gas pressure * Hydrogen gas purity * Generator ampere, voltage, and power   For further information see DCD [2] Section 10.2. |
| 4.68. | Each electrical battery room that contains batteries that could generate hydrogen during operation should be provided with an adequate ventilation system such that the hydrogen concentration is kept at a safe level below the lower flammability limit. The layout of the room and the design of the ventilation system should be such as to prevent local accumulations of hydrogen, with or without an operational ventilation system. | COM | The battery compartments are ventilated by a system that is designed to preclude the possibility of hydrogen accumulation. Therefore, a hydrogen explosion in a battery compartment is not postulated.  Each subsystem for the Class 1E battery rooms is provided with two 100 percent capacity supply air handling units, return/exhaust air fans, associated dampers, controls and instrumentation, and common ductwork.  Each non-Class 1E battery room is provided with an individual exhaust system to prevent the buildup of hydrogen gas in the room. Each exhaust system consists of an exhaust fan, an exhaust air duct and gravity back draft damper located in the fan discharge.  See DCD [2] Section 9.4.1.2.1.2 and Section 9.4.2.2.1.3. |
| 4.69. | Each electrical battery room should be provided with a hydrogen detection system and ventilation system sensors arranged to provide alarms in the main control room to indicate hydrogen levels approaching the lower flammability limit and any failure of the ventilation system. If fire dampers are installed on ventilation systems serving battery rooms, the effects of their closure on the buildup of hydrogen should be considered. In the event of an alarm, actions should be taken such as stopping battery charging. | COM | Nuclear island nonradioactive ventilation system and Annex/auxiliary buildings nonradioactive HVAC system are designed to maintain the hydrogen concentration in the battery rooms well below 2 percent by volume, as described in DCD [2] Sections 9.4.1 and 9.4.2. The battery rooms have hydrogen monitors that alarm in the MCR when the concentration is slightly below this value. |
| 4.70. | Consideration should be given to the use of recombinant batteries (which generate less hydrogen), but it should not be assumed that this will eliminate the risk of hydrogen production. | N/A | The type of batteries used in the AP1000 plant are lead-acid type storage batteries. The reason why lead-acid storage batteries are used is because no other battery technologies are currently qualified by the NRC for use in safety related electrical systems. Hydrogen concentrations are maintained as low as practicable with the use of dedicated and redundant ventilation systems.  See responses to Sections/Paragraphs 4.68 and 4.69. |
| 4.71. | The risk of explosions induced by fire exposure, such as boiling liquid expanding vapour explosions, should be minimized by means of separation between potential fires and potentially explosive liquids and gases, or by active measures such as suitable fixed fire suppression systems designed to provide cooling and vapour dispersion. | COM | The AP1000 plant safe distance for material in onsite storage facilities for explosions, flammable vapor clouds, and fires is tabulated in Table 2.2-1 in the DCD [2].  Equipment and facilities for fire protection, including detecting, alarming, and extinguishing functions, are provided to help protect both plant equipment and personnel from fire, explosion, and the resultant release of toxic vapors. Fire protection is provided by deluge systems (water spray), sprinklers, and portable extinguishers. |
| 4.72. | The provisions of paras 4.66, 4.67 and 4.77 should be applied, as appropriate, to the storage and use of any other bulk flammable gases. This should include cylinders containing flammable gases used in maintenance and repair work. | OR | The Owner shall be responsible for ensuring this requirement is met during operation and repair activities. |
| **MITIGATION OF THE EFFECTS OF EXPLOSIONS** | | | |
| 4.73. | Features that can resist or limit explosion effects (e.g. appropriate design or operating provisions) should be in place to minimize risks: examples are limiting the volumes of explosive gas mixtures, inerting, explosion venting (e.g. blow‑out panels or other pressure relief devices) and separation of explosion sources from items important to safety. Equipment that needs to maintain its functionality following a postulated initiating event should be identified and adequately designed to withstand the effects of the event, or to be protected against such events. | COM | Where an SSC supporting safety-related function can be affected by an internal explosion (e.g. the explosive material is supplied to the SSC so a leak could affect it), it is assumed that the whole train is disabled, together with any other SSC at that location. Safety-related function can still be provided by a redundant train protected by construction sufficiently robust to contain an explosion involving the maximum design quantity of explosive material.  A summary of mitigation measures is provided below:   * Only the quantities of potentially explosive materials necessary for operations are provided on site. * Where relatively large explosive quantities are required to be stored, these are located away from the buildings, at distances determined to be safe. An exclusion zone for structures near the liquid hydrogen storage facility has been determined to prevent any ignited release from progressing to a detonation. * Smaller quantities of potentially explosive materials are stored closer to where they are required. The locations have been determined to be safe with regard to the NI. * Piped hydrogen within the buildings is supplied from limited supplies, has a limited flow rate and passes through rooms sized or ventilated so that release of the maximum amount possible will not reach the LFL. * Potential ignition sources (permanent and temporary) are not permitted near enough to the hydrogen supply line that they would be in the temporarily potentially explosive region caused by a leak. * The battery rooms are ventilated so that hydrogen generated by charging does not exceed 2%. * Where processes may generate hydrogen, there are ventilation systems, hydrogen levels are monitored by fixed equipment, and equipment which can potentially be affected has segregated redundant equipment. |
| 4.74. | Consideration should be given to the blast overpressure and missiles generated by boiling liquid expanding vapour explosions, and to the potential for the ignition of flammable gases at a location distant from the point of release, which could result in the explosion of a gas cloud. The potential for boiling liquid expanding vapour explosions should be minimized by avoiding operation above the superheat limit temperature, as far as practicable. | COM | The AP1000 plant design considers internal explosions as described in DCD [2] Section 2.2 (Site-specific hazards, explosion by on-site storage facilities, flammable vapor clouds by on-site flammable liquids or gases). Missiles generated by explosions are considered in DCD [2] Section 3.5. |
| 4.75. | Some hazards (e.g. high energy arcing faults), while not formally explosions, are similar to explosions in terms of the loads they impart (e.g. temperature, pressure, missiles) on nearby SSCs; therefore, similar design provisions are appropriate for mitigating the effects of such hazards. | COM | Westinghouse takes care to provide protection against internal hazards throughout the plant area.  Suitable and sufficient design basis measures are identified such that an internal hazard, which may give rise to an explosion, does not prevent the delivery of the safety-related functions necessary to respond to a postulated event. Preservation of required safety functions ensures alignment with fault studies and structural integrity analysis. Within the AP1000 design, redundant divisions of safety-related SSC are segregated from one another such that a postulated hazards cannot result in the loss of all divisions. |
| 4.76. | Design provisions to limit the consequences of an explosion (overpressure, missile generation or fire) should be in place. The consequent effects of postulated explosions on items important to safety should be assessed against the design objectives in para. 2.12. Access routes and escape routes for operating personnel performing manual actions important to safety should also be assessed and special design provisions should be implemented, if necessary. | COM | See responses to Sections/Paragraphs 2.12, 4.73 and II.22. |
| 4.77. | Wherever there is a potential hazard due to hydrogen in plant operations, provision should be made to control the hazard by using hydrogen monitors, recombiners, adequate ventilation and controlled hydrogen burning systems (all of which should be designed for use in an explosive atmosphere), or other appropriate means. Where inerting is used, the fire hazard during operation periods without inert gas protection (e.g. maintenance and refuelling) should be considered, and care should be taken to ensure that gas mixtures remain within the limits of non‑flammability. | COM | The AP1000 plant includes onsite storage facilities for compressed and liquid hydrogen. Accidents involving accidental detonations of hydrogen from these storage facilities are evaluated as part of the AP1000 certified design.  The passive autocatalytic hydrogen re-combiners (PARs) are located within the containment. Hydrogen can be generated during design basis accidents by the reaction of a limited amount of zirconium in the Zircaloy fuel cladding with steam following a temporary core uncovery following large LOCAs; the purpose of the re-combiners is to convert the hydrogen back into water vapor, without the risk of an explosion. These work at relatively low hydrogen concentration and work under any conditions where hydrogen accumulates even during shutdown.  The primary means of containment atmosphere hydrogen analysis is the hydrogen analyzer described in DCD [2] Section 6.2.4.  Nuclear island nonradioactive ventilation system and Annex/auxiliary buildings nonradioactive HVAC system are designed to maintain the hydrogen concentration in the battery rooms well below 2 percent by volume, as described in DCD [2] Sections 9.4.1 and 9.4.2.  The gaseous radwaste system is designed to prevent hydrogen ignition both within its own boundaries and in connected systems (the liquid radwaste system and the nuclear island radioactive ventilation system). Containment Hydrogen Control System is described in DCD [2] Section 6.2.4. Plant Gas System is described in DCD [2] Section 9.32. Hydrogen Mixing and Combustion Analysis is described in DCD [2] Section 19.41. |
| **INTERNAL MISSILES** | | | |
| 4.78. | Nuclear power plants contain pressurized components and rotating machinery that can fail disruptively and cause missiles. A missile is an object that has kinetic energy and has left its design location. In this Safety Guide, the term internal missile is used to describe a moving object that originated from within the site boundary. | NR | This is a statement not a requirement. |
| **IDENTIFICATION AND CHARACTERIZATION OF MISSILE HAZARDS** | | | |
| 4.79. | Sources of possible missiles should be identified, and the likelihood, possible kinetic energy, size and trajectory of missiles should be estimated. The possible targets and the effects of missiles on items important to safety should be assessed. | COM | Missile protection is addressed in DCD [2] Section 3.5. Potential missiles due to failures of non-seismic items are addressed in DCD [2] Section 3.7.3.13. Heavy load-drop evaluations are described in DCD [2] Section 9.1.5.  The safety design approach adopted for the internal missile hazard within the AP1000 plant consists of a range of complementary approaches. These are applied as appropriate to individual items of equipment or systems to minimize the frequency of an internal missile occurring and then to minimize its potential to disrupt a safety-related SSC. The approaches adopted are as follows:   * Application of design codes to minimize the potential for a pressure part failure that could generate a missile. * Incorporation of design features in components to prevent missiles from being generated externally to the component. * Orientation of components, such as the main turbine, to direct any missile away from safety-related equipment. * Location of safety-related SSCs outside the zone of influence of a potential missile where practicable using either distance or separation by a structural barrier. |
| 4.80. | Analyses of missile hazards are usually performed by a combination of deterministic and probabilistic methods. Some missiles are postulated on a deterministic basis and their effects on SSCs in terms of strikes and damage are also evaluated. A formal description of the deterministic aspects of safety assessment should be presented, even in cases where all aspects of the missile hazard — initiation, strike and damage — are treated probabilistically. | COM | Missiles are deterministically assumed to occur as a result of a gross failure of SSCs, except those justified as Highest Safety Significance and those where valves are qualified to prevent missile generation. Missile protection is addressed in DCD [2] Section 3.5. |
| 4.81. | The potential for secondary missiles that could damage SSCs important to safety should also be evaluated. This evaluation should include consideration of potential fragment ricochet effects, if considered credible on the basis of expert judgement (e.g. the residual energy of the missile following impact can be judged sufficient to induce damage by ricochet when the robustness of targets in the vicinity is considered). | COM | Missile protection is addressed in DCD [2] Section 3.5. Potential missiles due to failures of nonseismic items are addressed in DCD [2] Section 3.7.3.13.   * Secondary Missiles Outside the Containment Building:   Falling objects (i.e. gravitational missiles) heavy enough to generate a secondary missile are postulated as a result of movement of a heavy load or from a nonseismically designed structure, system, or component during a seismic event. Movements of heavy loads are controlled to protect safety-related structures, systems, and components, see DCD [2] Section 9.1.5. Safety-related structures, systems, or components are protected from nonseismically designed structures, systems, or components or the interaction is evaluated. See DCD [2] Section 3.7.3.13 for additional discussion on the interaction of other systems with Seismic Category I systems. Valves, rotating equipment, vessels, and small fittings not otherwise considered to be credible missiles due to design features or other considerations are not considered to be a potential source of missiles when struck by a falling object. The outlet pipes and valves for the air storage bottles for the main control room are constructed to the ASME Code, Section III, requirements and are designed for seismic loads. The attached pipes and valves are not credible missile sources due to an accidental impact. The air storage bottles are located within a structural steel frame and are in an area with no activity directly above. For the reasons noted above, secondary missiles are not considered credible missiles.   * Secondary Missiles Inside the Containment Building:   Falling objects heavy enough to generate a secondary missile are postulated as a result of movement of a heavy load or from a nonseismically designed structure, system, or component during a seismic event. Movements of heavy loads are controlled to protect safety-related structures, systems, and components (see Section 9.1.5). Design and operational procedures of the polar crane inside containment precludes dropping a heavy load. Additionally, movements of heavy loads inside containment occur during shutdown periods when most of the high-energy systems are depressurized. Valves, rotating equipment, vessels, and small fittings not otherwise considered to be credible missiles due to design features or other considerations are not considered to be a potential source of missiles when struck by a falling object. Secondary missiles are not considered credible. Striking a component with a falling object will not generate a secondary missile if design of the component precludes generation of missiles due to pressurization of the component. Safety-related structures, systems, or components are protected from nonseismically designed structures, systems, or components or the interaction is evaluated. Nonsafety-related equipment that could fall and damage safety-related equipment during an earthquake is classified as seismic Category II and is designed and supported to preclude such failure. See DCD [2] Section 3.7.3.13 for additional discussion on the interaction of other systems with Seismic Category I systems. There are no high-pressure gas storage cylinders inside the containment shield building. For the reasons noted above, secondary missiles are not considered credible missiles. |
| **FAILURE OF PRESSURE VESSELS** | | | |
| 4.82. | In nuclear power plants, pressure vessels important to safety are designed and constructed by means of comprehensive and thorough practices to ensure their safe operation. Analysis is performed to demonstrate that levels of stress are acceptable under all design conditions. All stages of design, construction, installation and testing should be monitored in accordance with approved procedures to verify that all work is carried out in accordance with the design specifications and that the final quality of the vessel is acceptable. A surveillance programme during commissioning and operation, as well as a reliable system for overpressure protection, should be used to determine whether the vessels remain within their design limits. The gross failure of pressure vessels in nuclear power plants, such as the reactor pressure vessel or other high quality vessels designed with large margins, is, therefore, generally believed to be sufficiently improbable that consideration of the rupture of these vessels as an internal hazard is not necessary: see IAEA Safety Standards Series No. SSG‑56, Design of the Reactor Coolant System and Associated Systems for Nuclear Power Plants [9]. Failures of other vessels containing fluids of high internal energy should be evaluated, as they could become sources of missiles and other consequent hazards if they rupture. | COM  OR | Due to the conservative design, material characteristics, inspections, quality control during fabrication and erection, and prudent operation, failure of pressure vessels is reduced to a minimum.  Moreover, equipment for the AP1000 plant is selected to minimize the potential for missiles to be generated.  The AP1000 reactor pressure vessel and other important pressure vessels are designed, fabricated and inspected to the highest standards in accordance with the ASME Boiler and Pressure Vessel Code, Section III.  The Owner shall be responsible for the surveillance program during the operation. |
| 4.83. | As far as practicable, pressure vessels should be designed to fail in a ductile manner or in such a way that missiles and fragment hazards are reduced. If pressure vessels can possibly fail in a brittle manner, a range of missile sizes and shapes to cover the range of possibilities should be postulated and analysed to identify the missiles that determine the design basis of protective systems or structures. Alternatively, a simplified conservative approach is an acceptable way of determining the missiles to be considered. | COM | ASME Code, Section III vessel ruptures and ruptures of gas storage vessels constructed without welding using ASME Code, Section VIII criteria are not considered credible due to the conservative design, material characteristics, inspections, quality control during fabrication and erection, and prudent operation.  Vessels, Valves, rotating equipment, and small fittings not otherwise considered to be credible missiles due to design features or other considerations are not considered to be a potential source of missiles when struck by a falling object.  Failure of the reactor vessel, steam generators, pressurizer, core makeup tanks, accumulators, reactor coolant pump castings, passive residual heat exchangers, and piping leading to the generation of missiles is not considered credible. This is due to the material characteristics, preservice and inservice inspections, quality control during fabrication, erection and operation, conservative design, and prudent operation as applied to the particular component. |
| **FAILURES OF VALVES** | | | |
| 4.84. | Valves in fluid systems that operate with a high internal energy should be evaluated as potential sources of missiles. | COM | Equipment for the AP1000 plant is selected to minimize the potential for missiles to be generated. Missiles are postulated as described in DCD [2] Section 3.5.1.1.2. |
| 4.85. | Valve bodies are usually designed, constructed and maintained in such a manner that they are substantially stronger than the connected piping. For this reason, it is generally accepted that the generation of missiles resulting from the failure of the valve body itself is sufficiently unlikely that this need not be considered in the design and/or evaluation of the plant. | NR | This is a statement not a requirement. |
| 4.86. | The removable parts of a valve (e.g. stem, valve bonnet, motor) present the most significant potential for failures leading to the production of a missile, and this should be taken into consideration. | COM | The valve bonnets of pressure-seal, bonnet-type valves, constructed in accordance with ASME Code, Section III, are not considered credible missiles. The valve bonnets are prevented from becoming missiles by the retaining ring, which would have to fail in shear, and by the yoke capturing the bonnet or reducing bonnet energy. Because of the conservative design of the retaining ring of these valves, bonnet ejection is unlikely.  The valves of the bolted bonnet design, constructed in accordance with ASME Code, Section III, are not considered credible missiles. These bolted bonnets are prevented from becoming missiles by limiting stresses in the bonnet-to-body bolting material according to ASME Code, Section III requirements, and by designing flanges in accordance with applicable code requirements. Even if bolt failure would occur, the likelihood of all bolts experiencing simultaneous complete severance failure is not credible. The widespread use of valves with bolted bonnets, and the low historical incidence of complete severance failure of the bonnet, confirm that bolted valve bonnets are not credible missiles. Safety-relief valves in high energy systems use the bolted bonnet design.  Valve stems are not considered as credible missiles if at least one feature (in addition to the stem threads) is included in their design to prevent ejection. Valve stems with back seats are prevented from becoming missiles by this feature. In addition, the valve stems of valves with power actuators, such as air- or motor-operated valves, are effectively restrained by the valve actuator. Valve stems of rotary motion valves, such as plug valves, ball valves (except singleseat ball valves) and butterfly valves, as well as diaphragm-type valves are not considered as credible missiles. Because these valves do not have a large reservoir of pressurized fluid acting on the valve stem, there is little stored energy available to produce a missile. |
| **EJECTION OF A CONTROL ROD** | | | |
| 4.87. | For reactor designs in which there is significant fluid pressure in the reactor vessel, it has been customary to postulate the ejection of a control rod due to the driving forces of the fluid. Depending on the particular reactor design, this postulated missile could have the potential to cause significant primary or secondary damage. Typical concerns include the possible damage to adjacent control rods, to safety systems and to containment structures. | NR | This is a statement not a requirement. |
| **FAILURE OF HIGH SPEED ROTATING EQUIPMENT** | | | |
| 4.88. | The failure of the main turbine generator set, the steam turbines, large pumps (such as the main coolant pump) and their motors, or flywheels can result in the generation of missiles. Such failures can arise either from defects in the rotating parts or from excessive stresses due to overspeed. Typical missiles include the following: — Fan blades;  — Turbine disc fragments or blades; — Pump impellers;  — Fly wheels;  — Coupling bolts. | NR | This is a statement not a requirement. |
| 4.89. | Rotating machinery usually has a structure surrounding the rotating parts, and consideration should be given to the energy loss after failure due to the energy absorbing characteristics of the surrounding structure or casing. To the extent practicable, the calculation of the energy losses should be based on empirical data from tests of similar structures. For the sake of simplicity, an approach considering the interception of detached rotating parts by the casing could be applied based on operating experience feedback and manufacturer justifications. Alternatively, a conservative approach could be used in which it is assumed that no energy is lost in the interaction of the missile and the casing of rotating machinery. | COM | Rotating equipment is designed with surrounding housings to contain fragments in the event of failure i.e. the energy of rotating parts will be contained. Rotating components are protected against excessive over speed where appropriate, thus, minimizing the likelihood of disruptive failure. In addition, material characteristics, inspections, quality control during fabrication, erection and prudent operation contribute to reduce the likelihood of missile generation. Considerations about missiles generated by rotating machinery are described in DCD [2] Section 3.5. See also response to Section/Paragraph 4.90. |
| 4.90. | Missiles from the failure of rotating machinery should be characterized on the basis of their potential for damage and should be included in the evaluation of possible primary and secondary effects. Having identified the missiles to study, the potential direction of missiles should be characterized in terms of potential targets, taking into account the following:  (a) The maximum range of the missiles will be limited by the available energy and mass.  (b) Consideration of the directions in which missiles could be ejected should help in locating potential targets so as to avoid missile strikes, especially if the missiles are unidirectional (e.g. as for valve stems).  (c) In other cases, there could be a probable plane or angular sector for ejection of missiles, as is the case for rotating machines. There is evidence from failures of rotating machines that energetic missiles are usually ejected within a very narrow angle of the plane of rotation unless they are deflected by a barrier or stopped by the casing. However, there is also evidence that a small number of missiles could land in a wider angle from the plane of rotation. Therefore, sensitivity studies in relation to the direction of internal missiles, and the effect in terms of the site layout, might be necessary. | COM | Considerations about missiles generated by rotating machinery are described in DCD [2] Section 3.5. Within the internal missile safety case, the size and mass of the postulated rotating equipment projectile have been conservatively assumed to overpredict both the size and mass. Characteristics of impact, such as shape factors and the percent of mass converted into a missile, have been established with probability density functions and the frequency of occurrences. To eliminate possible ambiguity, and ensure further conservative results, the potential rotating equipment missile assumes that the full rotor/impeller will construct the postulated missile.  To prevent abnormal operation and failures by design, the material selection, design, build and verification requirements for a selection of SSCs ensure that the total energy contained in the rotating elements of the SSC is insufficient to move the mass of rotating parts so that it breaches the equipment housing. Therefore, a potential missile is retained within the SSCs equipment housing and does not result in a missile external to the SSC. |
| **PREVENTION OF MISSILE HAZARDS** | | | |
| **PREVENTION OF FAILURE OF PRESSURE VESSELS** | | | |
| 4.91. | Measures to prevent the failure of pressure vessels include the general considerations of the first level of defence in depth, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation. Regarding overpressure, specific measures relevant to pressure vessels include a reliable system for protection (e.g. safety relief valves, and the design of vessel anchors or supports). | NR | This is a statement not a requirement. |
| **PREVENTION OF FAILURE OF VALVES OR BOLTED CONNECTIONS** | | | |
| 4.92. | Valves should be designed to prevent removable parts from becoming missiles in the event of their failure. | COM | Equipment for the AP1000 plant is selected to minimize the potential for missiles to be generated. Missiles are postulated as described in DCD [2] Section 3.5.1.1.2. The following items are the major equipment selection considerations with regards to missile prevention:   * Valves that have only a threaded connection between the body and the bonnet are not used in high-energy systems. ASME Code, Section III valves with removable bonnets should be of the pressure-seal type or have bolted bonnets. * Valve stems of valves located in high-energy systems have at least two retention features. In addition to the stem threads, acceptable features include back seats on the stem or a power actuator, such as an air or motor operator. |
| 4.93. | As a design rule, no failure of a single bolt should lead to the generation of a missile other than the bolt itself. This recommendation applies to valves, pressure vessels and other bolted components with a high energy content. | COM | Valves of the bolted bonnet type are constructed in accordance with ASME Code, Section III. These valves are prevented from becoming missiles by limiting stresses in the bonnet to body bolting material according to ASME Code, Section III requirements, and by designing flanges in line with the applicable code requirements. Even if bolt failure was to occur, it is unlikely that all bolts would experience simultaneous complete severance failure. The widespread use of valves with bolted bonnets, and the low historical incidence of complete severance failure of the bonnet, confirm that bolted valve bonnets are not credible missiles. Safety relief valves in high energy systems use the bolted bonnet design. Valves that have only a threaded connection between the body and the bonnet are not used in high-energy systems. |
| 4.94. | Consideration should be given to the potential for multiple bolt failures due to corrosion or stress corrosion in the event of the leakage of fluid contents past gasketed joints. | COM | Equipment for the AP1000 plant is selected to minimize the potential for missiles to be generated. Even if bolt failure was to occur, it is unlikely that all bolts would experience simultaneous complete severance failure. |
| 4.95. | Unless this is precluded by other considerations, removable valve parts should be installed in such a manner that their ejection would not result in an impact of a missile on targets. | COM | As far as is practicable, removable valve parts are installed in such a manner that their ejection will not result in an impact of a missile on targets. |
| **PREVENTION OF CONTROL ROD EJECTION** | | | |
| 4.96. | The likelihood of a control rod being ejected should be reduced by providing special design features. This should be confirmed by a rigorous development programme to demonstrate that these features have the capability to retain the control rod and the drive assembly in the event of a failure of the travel housing for a control rod. | COM | Gross failure of a control rod drive mechanism housing, sufficient to create a missile from a piece of the housing or to allow a control rod to be ejected rapidly from the core, is not considered credible. This is because on the following reasons:   * The control rod drive mechanisms are shop hydrotested to 125 percent of system design pressure. * The housings are hydrotested to 125 percent of system design pressure after they are installed on the reactor vessel to the head adapters. They are checked again during the hydrotest of the completed reactor coolant system. * The housings are made of Type 304 or 316 stainless steel, which exhibits excellent notch toughness. * Stress levels in the mechanism are not affected by system thermal transients at power or by thermal movement of the coolant loops. * The welds in the pressure boundary of the control rod drive mechanism meet the same design, procedure, examination, and inspection requirements as the welds on other ASME Code, Section III, Class 1 components. * A nonmechanistic control rod ejection is considered in the safety analyses in DCD [2] Chapter 15 and the design transients in Section 3.9.1.1. |
| **PREVENTION OF FAILURE OF ROTATING MACHINERY** | | | |
| 4.97. | Proper orientation of rotating machinery should be considered as a preventive measure for major items such as the main turbine generator, both in terms of the orientation of the main shaft and the overall plant layout. The layout of the main turbine generator should be such that potential targets lie within the area least susceptible to direct strikes from missiles generated by turbine failure; that is, within a cone with its axis along the axis of the turbine shaft. This arrangement takes account of the fact that large sections of rotors, if ejected, will tend to be expelled in a direction perpendicular to the rotating shaft. A cone of ejection of 25° either side of perpendicular to the axis has generally been used as there is evidence that the majority of missiles are ejected within this cone; however, the designer should justify any such claim. The arrangement does not eliminate the possibility of such missiles hitting a target, but it significantly reduces the probability of a direct strike. | COM | The turbine and rotor design is described in the DCD [2] Section 10.2 and the turbine is oriented so that its shaft axis is perpendicular to the NI in which all of the safety-related SSCs are located. The orientation of the turbines is such that any low or high trajectory missiles generated are most likely to be ejected perpendicular to the axis of the turbine. The probability that a missile is directed away from the perpendicular decreases as the angle to the turbine axis decreases. Hence, it is extremely unlikely that fragments resulting from turbine disintegration would strike the NI structures. Safety-related SSCs are located outside of the low trajectory missile strike zone as defined in NUREG Guide 1.115. |
| 4.98. | The following approach should be taken to prevent the failure of rotating machinery:  (a) Careful selection of materials, speed control features and stress margins for all plant states considered in the design basis.  (b) Non‑destructive examination and other testing to detect possible defects, and quality control measures to ensure that the equipment as installed meets all specifications.  (c) Evaluation of the reliability of the means of preventing destructive overspeed. This should include equipment for the detection and prevention of overspeed, associated power supply equipment and instrumentation and control equipment, as well as the procedures involved in the periodic calibration and readiness testing of this equipment. | COM  OR | Rotating equipment is designed with surrounding housings to contain fragments in the event of failure i.e. the energy of rotating parts will be contained. Rotating components are protected against excessive over speed where appropriate, thus, minimizing the likelihood of disruptive failure. In addition, material characteristics, inspections, quality control during fabrication, erection and prudent operation contribute to reduce the likelihood of failure.  The Owner shall be responsible for conducting the appropriate tests and implementing procedures. |
| 4.99. | Additional redundant means of limiting the rotational speed should be provided by such features as governors, clutches and brakes, and by a combination of systems for instrumentation, control and valving to ensure that the likelihood of overspeed occurring is acceptably low. | COM | Rotating components are protected against excessive over speed where appropriate, thus, minimizing the likelihood of disruptive failure.  Reactor coolant pump design requirements are established so that any failure of the rotating parts would be retained within the casing at specified overspeed conditions. This is discussed in DCD [2] Section 5.4.1.3.6.  Turbine over speed protection systems are incorporated into the design. |
| 4.100. | Although engineering solutions are available to limit speed and to prevent missiles due to excessive overspeed, these provisions by themselves might not make the probability of missiles being generated from rotating equipment acceptably low. In addition to the failure caused by overspeed there is also the possibility of a flaw in the rotor resulting in missiles being generated at or below normal running speed. These missiles should be addressed by other means, such as conservative design, high quality manufacturing, careful operation, appropriate monitoring of parameters (such as vibration) and comprehensive in‑service inspection. Rotating plant equipment should be maintained and replaced in accordance with manufacturers’ instructions. When all these means are properly used, the probability of missiles being generated through the failure of rotating machines can be significantly reduced. | COM  OR | See response to Section/Paragraph 4.98.  The design specification for rotating equipment requires compliance with ASME Code, Section III or ANSI codes or the Hydraulic Institute Standards. For smaller pieces of equipment such as sample pumps, the requirements are limited to manufacturers’ standards as the items are small and are not in high energy systems.  The Owner shall be responsible for conducting the appropriate inspections. |
| **MITIGATION OF THE EFFECTS OF MISSILE HAZARDS** | | | |
| 4.101. | Features that can retain energetic missiles resulting from the failure of equipment, or that will deflect such missiles towards a harmless direction, should be considered in the design. | COM | The plant is designed such that it can be operated with sufficient levels of protection in place to ensure that internally generated missiles will not prevent delivery of safety functions. This defense in depth is provided by:   * The conservative design of equipment, the manufacture, maintenance, and operation of that equipment in accordance with safety margins (through compliance with recognized design codes) appropriate engineering practices and monitoring of the quality of these aspects. * Use of structural barriers to limit the path of any missile generated to areas where damage will not prevent the delivery of safety functions. * Sufficient redundancy and defense in depth is provided to ensure that even if there is the loss of any SSC as a result of an internally generated missile the safety function can still be delivered. |
| 4.102. | To control missiles close to their potential source, valves, pumps, motor generators and high pressure gas containers should be located in areas with barriers such as an adequately strong concrete structure. Targets can also be protected by barriers. Barriers are also used to reduce certain secondary effects such as scabbing or the ejection of concrete blocks from concrete targets. | COM | The consequences of missile generation are mitigated through the provision of segregation barriers that can withstand the impact of possible missiles such that the safety functions and post-72 hour functions are not compromised. Additionally redundant safety equipment is segregated by distance from the missile source. |
| 4.103. | Usually, missile barriers consist of reinforced concrete slabs or of steel plates. However, other means such as woven steel mats or missile deflectors can also be used. | NR | This is a statement not a requirement. |
| 4.104. | In the design of barriers, both local and general effects of missiles on the barriers should be considered, as follows:  (a) Concrete and reinforced concrete barriers:  (i) The design of concrete barriers should ensure that the barriers will not collapse under the missile impact. Therefore, the thickness and the strength of the barriers should be conservatively defined, consistent with the possible mass, kinetic energy, location of impact and type of missiles (hard missile, soft missile).  (ii) Elastoplastic, ductile behaviour of the barrier is allowed.  (iii) The design of the barriers should ensure that hard missiles will not penetrate the barrier.  (iv) There should be an analysis to ensure that missiles will not cause scabbing or spalling at the safe side of the barrier, and that concrete fragments will not impact SSCs important to safety.  (v) The generation of secondary missiles from concrete barrier fragments should be avoided by multi‑layer or composite barriers.  (vi) Analysis of the penetration depth and of spalling and scabbing phenomena can be performed using empirical formulas or other analytical models as appropriate.  (b) Steel and multi‑layer composite barriers:  (i) The design of these barriers should be based on empirical formulas for penetration or other analytical models as appropriate.  (ii) The overall deformation of steel or composite barriers should not result in the loss of barrier function, and the deformed barrier should not impact on the SSCs to be protected.  (c) Vibratory effect:  (i) The vibratory response of the barrier to missile impact should be considered as a secondary effect that could have adverse effects on the SSCs to be protected. | COM | See DCD [2] Section 3.5.3 (“Barrier Design Procedures”). Missile barriers and protective structures are designed to withstand and absorb missile impact loads to prevent damage to safety-related components. Such passive protective measures have been incorporated in the AP1000 plant design to protect safety-related SSCs and post 72-hour functions from internal missile faults. In this regard, the consequences of missile hazards are contained through the use of passive barriers, thus limiting impacts to, and loss of, a safety function. |
| **CASES WITHOUT PROTECTION BY SPECIFIC MISSILE BARRIERS** | | | |
| 4.105. | In some cases, it will not be necessary to provide specific missile barriers. For example, the missiles could be of relatively low mass and energy, and the targets could be sufficiently strong to withstand them, even without additional protection. The boundaries of existing buildings might limit missile effects on the plant. Detailed analysis of the potential impact on the target should be performed to demonstrate that the impact and its potential secondary effects do not affect SSCs important to safety. Physical separation of the redundant safety systems will also ensure that safety functions continue to be performed even if missiles damage components of one or more of the redundant safety systems. | COM | The likelihood of loss of safety-related SSCs as a result of an internally generated missile is extremely small and has been addressed in the design of the plant and by normal operational procedures. Specific measures taken to reduce risk include:   * Equipment that has the potential to generate missiles is designed, manufactured, and maintained to fulfil the requirements of identified design standards so minimizing the probability of actually generating internal missiles. * If a missile is generated, then the structures surrounding the source of the missile ensure that the safety-related SSCs in adjacent areas are protected by the surrounding structures acting as barriers or through them being placed such that missiles will not reach safety-related SSCs outside of the area. * Where protection is not possible for functional reasons, sufficient diversity and redundancy exists that the safety function can still be delivered. |
| **MITIGATION OF THE CONSEQUENCES OF MISSILES DUE TO RUPTURE OF PRESSURE VESSELS** | | | |
| 4.106. | Modes of failure of a pressure vessel will depend upon a variety of parameters, including the design, the materials of construction, weld details, quality control in manufacture and operating conditions. It is highly unlikely that the vessel as a whole could become a missile, especially if it is well restrained. With some vessels, dome end failure might lead to the largest potential missile. Depending on the vessel and operating conditions, a more fragmentary failure could also be possible. To develop protective measures against missiles, attention should be paid in the safety assessment to characterization of potential missiles from the particular vessel and the effects of these missiles on the plant and structures local to the vessel. | COM | Equipment for the AP1000 plant is selected to minimize the potential for missiles to be generated. Due to the conservative design, material characteristics, inspections, quality control during fabrication and erection, and prudent operation, failure of pressure vessels is reduced to a minimum.  The conservative approach is taken as based on the assumption that all stored energy within the vessel is converted into kinetic energy and applied to the largest missile mass possible, i.e., the entire tank. The potential effects of missiles on structures have been evaluated. |
| 4.107. | The provision of an unpressurized guard pipe around certain sections of piping carrying high pressure fluids could, in some cases, be useful for protection against missiles. Two protection features are provided: protection of the surrounding structures and equipment from whipping pipes and possible secondary missiles, and protection of the inner pipe from missiles generated in the surrounding area. Consideration should be given to the potential for release of fluid from the impacted pipe and the resulting internal flood. | COM | Guard pipes are designed for pipe rupture protection. Guard pipes in the containment annulus areas of the break exclusion zones are designed according to the rules of Class MC, subsection NE, of the ASME Code. Level C service limits of the ASME Code, Section III, Paragraph NE-3221(c), (see DCD [2] Section 3.9.3) are not exceeded by the loadings associated with containment design pressure and temperature in combination with a safe shutdown earthquake. The guard pipe assemblies are subjected to a pressure test performed at the maximum operating pressure of the enclosed process pipe. Other guard pipes are designed and constructed to the same ASME rules as the enclosed process pipe.  Guard pipes in the break exclusion zones provide additional confidence that pipes will not leak into the annulus between the containment vessel and the shield building. |
| **MITIGATION OF THE CONSEQUENCES OF MISSILES DUE TO RUPTURE OF VALVES** | | | |
| 4.108. | Features that can retain energetic missiles resulting from the rupture of valves, or that will deflect such missiles towards a harmless direction, should be considered in the design. This could include walls or local missile barriers. | COM | The consequences of missile generation are mitigated through the provision of segregation barriers that can withstand the impact of possible missiles such that the safety functions and post-72 hour functions are not compromised. Additionally redundant safety equipment is segregated by distance from the missile source.  The civil engineering structures provide structural support to the SSCs but also act as suitable barriers for a number of functions, including preventing accidentally generated missiles from travelling to a location where significant harm could occur. |
| **MITIGATION OF THE CONSEQUENCES OF MISSILES DUE TO FAILURE OF ROTATING MACHINERY** | | | |
| 4.109. | Features that can retain energetic missiles resulting from the failure of rotating machinery, or that will deflect such missiles towards a harmless direction, should be considered in the design. | COM | See response to Section/Paragraph 4.108. |
| **PIPE BREAKS (PIPE WHIP AND JET EFFECT AND FLOODING)** | | | |
| **IDENTIFICATION AND CHARACTERIZATION OF PIPE BREAKS** | | | |
| 4.110. | Depending on the characteristics of the pipes under consideration (internal parameters, diameter, stress values, fatigue factors), the following types of failure should be considered:  (a) High energy pipes7 can suffer from circumferential rupture or longitudinal through‑wall crack, or both. The high energy of the contained fluid means that dynamic effects, such as pipe whip or jet impingement, are important and should be considered.  (b) Low energy pipes can also suffer through‑wall cracks, either longitudinal or circumferential, although, given the energy of the fluid, such cracks would generally be more stable than those in high energy pipes, and dynamic effects would be less significant. By exception, for low energy pipes, it could be possible to justify limiting the leak size to an area significantly smaller than their inner cross‑section.  **\_\_\_\_\_\_\_\_\_\_**  7 In some States, a high energy pipe is defined as a pipe with an internal operating pressure of more than 1.9 MPa or an operating temperature of more than 95°C in the case of water. In other States, these limits are 2.0 MPa and 100°C respectively. Other limits may apply for other fluids, for example gas at greater than atmospheric pressure. | COM | The AP1000 plant pipe failure protection program is generally in compliance with 10 CFR 50, Appendix A, General Design Criterion 4, ANS-58.2-1988, Standard Review Plan Section 3.6.1, 3.6.2, and NUREG-1061 Volume 3. High energy and moderate energy lines are defined by pressure and temperature criteria. Table 3.6-1 in DCD [2] identifies systems which contain high and moderate-energy lines. See also DCD [2] Section 3.6 (“Pipe Breaks”) and Appendix 3B (“Leak before break criteria”). |
| 4.111. | It may be acceptable to postulate only a limited leak (and not a break), if it can be demonstrated that the piping system considered is operated under ‘high energy’ parameters for a short period of time8 (e.g. less than 2% of the total operating time). Some States have identified criteria for excluding certain pipe segments from break analysis (see para. 4.136). Alternatively, an assessment of the consequences assuming a full pipe break can be viewed as a good practice to demonstrate the robustness of the design.  **\_\_\_\_\_\_\_\_\_\_**  8 This approach is considered acceptable only in some States | NR | This is a statement not a requirement. |
| 4.112. | Failure should be postulated at the following locations:  (a) At the terminal ends (fixed points, connections to a large pipe or to a component) and at welds and intermediate points of high stress for a piping system designed and operated in accordance with the rules applied for safety systems. Other locations of this piping system, where a piping failure would lead to bounding effects on SSCs important to safety, should be verified, possibly using realistic assumptions.  (b) In all locations for other pipes. | CWO | Section 3.6.2 in the DCD [2] defines the criteria for postulated break location and configuration. For pipes with a nominal diameter of:   * 4 inches or greater: Failures are postulated only at terminations and at intermediate locations where the pipe stressing or fatigue duty is significant. Branch connections are regarded as terminations and, at terminations, only circumferential cracks are assumed. * Greater than 1 inch but less than 4 inches: Only circumferential breaks are postulated at each selected break location. * 1 inch or less: No breaks are postulated. |
| 4.113. | For small9 diameter piping systems, which are sensitive to vibration induced failure and to rupture due to external forces, breaks should be postulated at any location.  **\_\_\_\_\_\_\_\_\_\_**  9 Some States have defined ‘small’ as a pipe with a nominal diameter of 50 mm or less. In other States, pipes with nominal diameter of 25 mm or less are considered small. | CWO | See response to Section/Paragraph 4.112. |
| 4.114. | A circumferential pipe rupture might result from damage due to a degradation mechanism, such as corrosion or fatigue (i.e. a crack growing over its critical size), or due to an acute overload (e.g. by water hammer or impact due to the rupture of other piping). The most probable location of such a pipe rupture is any circumferential weld between the straight pipe parts and the pipe components such as pipe bends, T intersections, reducers, valves or pumps. In general, pipe rupture should be considered at any location where there are changes in stiffness and vibration or fluid stratification caused by temperature differences. | COM | Section 3.6.2 in the DCD [2] defines the criteria for postulated break location and configuration. |
| 4.115. | The estimated frequency of a double ended guillotine break of high energy piping should be derived from operating experience or from fracture mechanics calculations. This frequency might also be available from evaluations performed for the purposes of probabilistic safety assessment. | COM | Double-ended guillotine breaks are assumed for pipe ruptures, and catastrophic tank, valve, and pump ruptures are also assumed as the component failures that would result in flooding. See Chapter 56 and Appendix A in PRA [4]. |
| 4.116. | If longitudinal welds are present in high energy piping, a large longitudinal through‑wall crack resulting in a break or large leakage area should be considered. | COM | Section 3.6.2 in DCD [2] defines the criteria for postulated break location and configuration. High-energy pipes are evaluated for the effects of circumferential and longitudinal pipe breaks and through-wall cracks. |
| 4.117. | Complete instantaneous breaks of high energy pipes should be postulated when analysing local effects on SSCs important to safety, such as direct mechanical contact (pipe whip) or jet impingement including potential blast wave load. Furthermore, the global effects10 of breaks in these pipes, including consequences such as flooding, increases in humidity, increases in temperature and higher radiation levels, should be taken into consideration when designing the supports, the protection means (e.g. pipe restraints) and the relevant SSCs important to safety.  **\_\_\_\_\_\_\_\_\_\_**  10 In the context of this Safety Guide, ‘global effects’ refers to possible effects across the entire site. | COM | Pipe failure protection is provided according to the requirements of 10 CFR 50, Appendix A, General Design Criterion 4. In the event of a high- or moderate-energy pipe failure within the plant, adequate protection is provided so that essential structures, systems, or components are not impacted by the adverse effects of postulated piping failure. Essential systems and components are those required to shut down the reactor and mitigate the consequences of the postulated piping failure. Nonsafety-related systems are not required to be protected from the dynamic and environmental effects associated with the postulated rupture of piping except as described in DCD [2] Section 3.6.1.1, item Q.  Analysis methods and criteria for evaluating pipe whip and evaluating the consequences of jet impingement, motions of the pipe, and system depressurization on integrity and operability are provided.  Section 3.11 in the DCD [2] discusses the qualification of the equipment required to function in the adverse environmental conditions including temperature, humidity, pressure, and chemical consequences. |
| 4.118. | Pipe failures could have an impact on SSCs important to safety by means of the local and global effects described in para. 4.117. All these possible effects should be analysed and considered in the plant design, in particular for protective and mitigatory measures. | COM | Section 3.6.1 in DCD [2] provides the design bases and criteria for the analysis required to demonstrate that essential systems are protected. The high- and moderate-energy systems representing the potential source of dynamic effects are listed. Additionally, the criteria for separation and the effects of adverse consequences are defined. See also response to Section/Paragraph 4.117. |
| 4.119. | Three main phenomena that could be induced by pipe failures are pipe whip, jet effects and flooding. The first two phenomena are addressed in paras 4.120–4.144, and internal flooding is addressed in paras 4.145–4.172. Secondary effects such as failure induced missiles and the environmental effects of the break (e.g. local increase in temperature and pressure) are also addressed. | NR | This is a statement not a requirement. |
| **PIPE WHIP** | | | |
| 4.120. | Pipe whip in its usual form occurs as a consequence of a double ended guillotine type pipe break in high energy piping. As the free cross‑sections of the broken pipe are propelled by the forces of the discharging high energy fluid, they are accelerated, which tends to move them from their installed configuration. In the case of sufficiently large movement of the pipe branch, the increasing bending moment could cause plastic deformation and the formation of a plastic hinge at the nearest pipe whip restraint or at a rigid (or sufficiently stiff) support. This defines the length of the pipe branch that rotates coherently about this point during the phase of free pipe whip movement. | NAR | This is a statement not a requirement. |
| 4.121. | For assumed breaks where the full lengths of both pipe segments are at the same elevation, the pipe whip should be assumed to occur only at the same elevation; otherwise, motion in all directions (i.e. a sphere centred on the plastic hinge) should be assumed. | COM | Pipe whip is assumed to occur in the plane defined by the piping geometry and to cause movement in the direction of the jet reaction. Measures for protection against pipe whip are provided where the unrestrained pipe movement of either end of the ruptured pipe could cause damage at an unacceptable level to any structure, system, or components. Protection against the dynamic effects associated with the postulated rupture of piping is described in DCD [2] Section 3.6. |
| 4.122. | In the case of a large longitudinal through‑wall crack in high energy piping, no classical pipe whip occurs in the vicinity of this break since there is no separation of the pipe. However, large displacements should be considered, on the basis of the assumption that the piping forms a V shape with three plastic hinges and has the potential to affect other nearby equipment. | COM | Pipe whip restraints are generally located so that a plastic hinge does not form in the pipe. If, because of physical limitations, pipe whip restraints are located so that a plastic hinge can form, the consequences of the whipping pipe and the jet impingement effect are further investigated. Pipe whip restraints are designed and located with sufficient clearances between the pipe and the restraint in such a way that they do not interact and cause additional piping stresses. See Section 3.6.2 in the DCD [2]. |
| 4.123. | The whipping pipe branches should be analysed geometrically to determine possible directions of motion that might endanger target SSCs. In addition, the analysis should include an assessment of the effectiveness of the pipe whip restraints, demonstrating that pipe deflections would be limited by the physical restraints. In the case of terminal end breaks, consideration should be given to the secondary effects on the remaining terminal ends. | COM | Analysis and design criteria of pipe whip restraints for postulated pipe break effects are consistent with the guidelines in ANSI/ANS-58.2-1988 [18]:   * Pipe whip restraints are designed based on energy absorption principles by considering the elastic-plastic, strain-hardening behavior of the materials used. * Non-energy absorbing portions of the pipe whip restraints are designed to the requirements of AISC N690 Code supplemented by the requirements given in the Section 3.8.4.5 DCD [2]. * A rebound factor of 1.1 is applied to the jet thrust force. * Except in cases where calculations are performed to verify that a plastic hinge is formed, the energy absorbed by the ruptured pipe is conservatively assumed to be zero. That is, the thrust force developed goes directly into moving the broken pipe and is not reduced by the force required to bend the pipe. * Other structural members of the pipe whip restraints are designed for elastic response. A dynamic increase factor is used for those members that are designed to remain elastic. * The criteria for allowable strain in a pipe whip restraint are dependent on the type of restraint. |
| 4.124. | For the analysis of the consequences of an impact, it should be assumed that any impact of a whipping pipe onto a pipe of similar design but smaller diameter results in damage (a break) to the target pipe. Subject to justification, impacted target pipes of a diameter equal to or larger than that of the impacting pipe need not be assumed to lose their integrity. However, if an additional mass (such as a valve or an orifice plate) is present on the whipping branch, the kinetic energy of the motion is increased. Additionally, the stiffness of the pipe — and therefore its capacity to damage a larger pipe — might increase if there is a change in pipe shape (e.g. an elbow) near the end of the pipe. In these cases, the target pipe could be broken even if it is larger than the whipping pipe. Cables and cable trays and different types of structure and instrumentation should be considered as possible targets if they support systems or components important to safety. | COM | Where pipe whip would have the potential to cause the failure of a safety-related SSC then mitigations have been provided in the form of restraints, shielding, barriers and separation.  Appendix B of the Pipe Rupture Protection Design Criteria [19], addresses the methods for the analysis and mitigation of: thrust force at postulated breaks; pressure transient inside the postulated broken pipe; jet impingement from postulated breaks; and pipe whip as a result of postulated breaks.  Missile impact load on a structure generated by or during the postulated break, as from pipe whipping, as described in DCD [2] Section 3.6 |
| 4.125. | In the investigation of the whipping pipe, consideration should be given to the potential for a subsequent break after an impact on a target, with the ejection of secondary missiles. Sources of missiles could be single concentrated masses within or attached to a pipe branch, such as valves and pumps. If these components have separate supports that are designed to prevent such breaks and the formation of secondary missiles, the analysis should be extended to these anchor points. Attention should also be paid to instrumentation wells and similar attachments to the pipe as further possible sources of missiles. | COM | Missile impact load on a structure generated by or during the postulated break, as from pipe whipping, as described in DCD [2] Section 3.6 See also response to Section/Paragraph 4.81. |
| **JET EFFECTS** | | | |
| 4.126. | A jet is a stream of fluid ejected from a leak or break in a pressure retaining system, in a particular direction and with a significantly high velocity. | NR | This is a statement not a requirement. |
| 4.127. | Jets usually originate from a broken component, such as a pipe or vessel, containing high energy pressurized fluid. Jets can be excluded from consideration for low energy systems. | NR | This is a statement not a requirement. |
| 4.128. | The origin of the jet is usually assumed to be a circumferential or longitudinal break of a vessel or pipe. The resulting jet is then limited to a particular direction. In the case of circumferential breaks, the jet is assumed to be oriented axially with respect to the pipe. In the case of longitudinal breaks, the jet is assumed to be oriented radially. | NR | This is a statement not a requirement. |
| 4.129. | Other possible sources of jets should be considered, where appropriate. An example of such a source is a jet of gas (the possible effects of the ignition of this gas are considered in paras 4.1–4.77). | COM | All credible sources of jets have been considered. See DCD [2] Chapter 3 and Chapter 19. |
| 4.130. | For each postulated location and size of break, the jet geometry (shape and direction) and its physical parameters (e.g. pressure, temperature, density) should be evaluated as a function of time and space. | COM | Jet parameters, volumetric area of affected compartments, plant layout, and separating structures are considered. Parameters that determine the shape of the jet and the magnitude of the jet and thrust loads include pressure, temperature, and friction losses between the break and the reservoir. The volumetric area affected is determined by considering jet shape and loads at the postulated location of the breaks. See DCD [2] Section 3.6. |
| 4.131. | If the break generates more than one jet, the possible interference of the jets should be taken into account. This is the case for a double ended break of a pipe without restraints, in which two jets could be generated, one from each of the broken ends of the pipe. | COM | All credible jet sources have been considered in case of failure. |
| 4.132. | The effect of the motion of the jet’s source (such as a whipping pipe) on the jet’s geometry should be taken into account, as well as other possible effects (such as those due to objects in the vicinity of the jet’s trajectory). | COM | The effect of the movement of the jet’s source is taken into account. |
| 4.133. | A conservative analysis, using either an appropriate and verified computer model or a simplified approximation on the basis of experimental data, or other appropriate and justified conservative assumptions, can be used for the analysis of the jet’s shape and other properties. | NR | This is a statement not a requirement. |
| 4.134. | The following effects of jets on targets should be taken into account: mechanical load (pressure, impact), thermal load (temperature, including thermal stresses and shocks where appropriate) and properties of fluids (such as possible short circuits in electric equipment due to the conductivity of liquid water). Possible chemical effects should also be evaluated, particularly if the fluid ejected is not water. | COM | The consequences were considered in a broad sense. See DCD [2] Section 3.6.2.2. |
| 4.135. | It might be necessary to analyse the effects of jets on targets that are not SSCs important to safety if their damage might lead to significant secondary consequences. A typical example is damage to pipe insulation inside the containment. Although the insulation itself is not important to safety, debris from insulation material could block the emergency core cooling or containment spray sump strainers during recirculation cooling. Relevant recommendations are provided in paras 4.84 and 4.85 of IAEA Safety Standards Series No. SSG‑53, Design of the Reactor Containment and Associated Systems for Nuclear Power Plants [10]. | NR | This is a statement not a requirement. |
| **PREVENTION OF PIPE BREAKS** | | | |
| 4.136. | In some States, it has been judged that the application of very high quality standards for high energy piping, similar to those for vessels, could reduce the risk of pipe breaks to such a low level that it can be effectively excluded from further consideration. Some States have identified criteria for excluding certain pipe segments from break analysis (see, for example, Ref. [11]). | NR | This is a statement not a requirement. |
| 4.137. | For locations where break preclusion criteria are met, a leak (rather than a complete rupture) may be assumed.11 To determine the leak size, a fracture mechanics analysis should be performed. Alternatively, a crack corresponding to a leak size of 10% of the flow cross‑section should be postulated. The leak detection system should be shown to have a sensitivity that is adequate to detect the minimum leakage from a crack of this size.  **\_\_\_\_\_\_\_\_\_\_**  11 This is applicable in States where the leak before break concept has been accepted. | COM | The methods and criteria to evaluate leak-before-break in the AP1000 plant are consistent with the guidance in NUREG-1061 [20] and Draft Standard Review Plan 3.6.3 [21]. Leak-before-Break Evaluation Procedures are described in DCD [2] Section 3.6.3. |
| 4.138. | For all piping, the likelihood of a pipe break can be reduced significantly if safety measures are applied, notably for design, manufacturing, construction and surveillance (increased in‑service inspections or monitoring for leakage, vibration and fatigue, water chemistry, loose parts, displacements, and erosion and corrosion). | NR | This is a statement not a requirement. |
| **MITIGATION OF THE CONSEQUENCES OF PIPE BREAKS** | | | |
| **MITIGATION OF THE CONSEQUENCES OF PIPE WHIP** | | | |
| 4.139. | The likelihood of a severe pipe rupture in the piping systems of a nuclear power plant is generally accepted to be low; however, pipe restraints should be used to restrict the motion of pipes that, if broken, could impact SSCs important to safety. | COM | Pipe whip restraints are provided wherever postulated pipe breaks could impair the capability of any essential system or component to perform its intended safety functions. Section 3.6.2.3 in DCD [2] gives the design criteria for and description of pipe whip restraints. See also Section 3.6.1.3.2 in the DCD [2]. |
| **MITIGATION OF THE CONSEQUENCES OF JETS** | | | |
| 4.140. | If a high energy pipe does break, the generation of a jet cannot be avoided; the only way to prevent the generation of a jet is to prevent the break itself. However, means of limiting the jet in time and/or space should be considered. For example, valves installed upstream and check valves installed downstream of the point of failure can stop the jet soon after it is initiated. Robust barriers (e.g. concrete walls) around the failed pipe should be used to limit the range of the jet. | COM | Barriers and shields, constructed of either steel or concrete, are provided to protect essential equipment, including instrumentation, from the effects of jet impingement resulting from postulated pipe breaks. Barrier and shield design is based on elastic methods and the elastic-plastic methods for dynamic analysis included in Biggs, J. M. [22]. Design criteria and loading combinations are according to Sections 3.8.3 and 3.8.4. See Section 3.6.2.4.1 in the DCD [2]. Essential equipment protected by pipe whip restraints or jet shields is listed in the DCD [2] Table 3.6-3. |
| 4.141. | To the extent practicable, coatings and insulation materials that are resistant to jet impingement should be used to limit the amount of debris that is generated by the jet (since this debris can challenge the performance of safety systems under certain conditions). | COM | Coatings and insulation materials that are resistant to jet impingement are used where necessary. |
| **SPECIFIC JET HAZARD CONSIDERATIONS** | | | |
| 4.142. | In addition to the direct impingement of a jet onto targets (local effects), the release of fluid from a leak or break could also have a significant effect on the general environmental conditions in a room. The effects will depend, among other things, on the time duration and the parameters of the jet and on the dimensions of the room. If this is a concern, then the general environmental parameters and their influence on SSC functionality should also be analysed and included in the environmental qualification process. | COM | Section 3.11 in the DCD [2] discusses the qualification of the equipment required to function in the adverse environmental conditions including temperature, humidity, pressure, and chemical consequences. |
| 4.143. | The effect of a differential pressure across a structure or portion of a structure (e.g. a wall), for example due to the steam released by a break, should be considered when designing the plant. Blow‑out panels and doors that open when subjected to a certain pressure or temperature are examples of measures that can be used to mitigate this effect. | COM | The effect of a differential pressure across a structure or portion of a structure has been considered. |
| 4.144. | Protection against direct jet impingement is similar to protection against missiles. Protective measures should be designed in such a way as to cope with both missiles and jets, or generally with as many internal hazards as practicable. | COM | The plant arrangement is based on maximizing the physical separation of redundant or diverse safety-related components and systems from each other and from nonsafety-related items.  Protection requirements are met through the protection afforded by walls, floors, columns, abutments, and foundations. Where adequate protection does not already exist as a result of separation, a separating structure such as additional barriers, deflectors, or shields is provided to meet the functional protection requirements. Barriers and shields, constructed of either steel or concrete, are provided to protect essential equipment, including instrumentation, from the effects of jet impingement resulting from postulated pipe breaks.  See Section 3.6.2.4.1 in the DCD [2]. |
| **INTERNAL FLOODING** | | | |
| **IDENTIFICATION AND CHARACTERIZATION OF INTERNAL FLOODING HAZARDS** | | | |
| 4.145. | Internal flooding can be caused by any event that results in the release of a liquid (usually water12) that exceeds the drainage capacity in a given area. Flooding can affect multiple SSCs (i.e. those that are not designed to withstand being submerged or exposed to spray). Although the guidance in this subsection is limited to internal flooding, external events (e.g. earthquake, external flooding) can cause or exacerbate internal flooding.  **\_\_\_\_\_\_\_\_\_\_**  12 This subsection addresses water based flooding; however, the same considerations apply to other liquids on the site if they exist in sufficient quantities and locations that could cause a flood. Possible examples include fuel, chemicals and fire extinguishing materials. | NR | This is a statement not a requirement. |
| 4.146. | Flooding means not only the formation of pools of water on the floor of a room but also the collection of water in higher locations. For example, water (arising from sprays or condensed steam) could collect in cable trays even if they are located well above the floor level. Equipment located in such a place should then be considered to be subject to flooding. In addition, water from these trays might be drained to other locations where its presence is also undesirable. | COM | Flooding as an internal hazard has been addressed in the AP1000 plant design as described in DCD [2] Sections 3.4 and 19.56. Protection from internal flooding has been described in the AP1000 DCD [2] in Section 3.4.1.1.2. Evaluation of internal flooding has been described in the AP1000 DCD [2] in Section 3.4.1.2.2. Water collection at higher locations has been considered and appropriate preventive measures have been implemented in the design. |
| 4.147. | Actions undertaken by plant personnel (e.g. maintenance activities) that can lead to flooding should be considered. | COM | Human factors are described in DCD [2] Chapter 15 and Chapter 18. |
| 4.148. | Examples of events that could cause a flood include the following:  (a) A leak or break in the primary or secondary coolant system;  (b) A leak or break in the emergency core cooling system;  (c) A leak or break in the service water system;  (d) A leak, break or spurious operation of the fire extinguishing system;  (e) Human error during maintenance (e.g. leaving a valve, an access hole or a flange open by mistake);  (f) A leak in piping systems such as the domestic water, circulating water or condensate systems or water from outside entering the plant through drains. | NR | This is a statement not a requirement. |
| 4.149. | All possible flooding hazards should be systematically identified. One approach is to list SSCs and then to identify all the possible sources of water (including sources in other rooms) and systematically identify the flood propagation pathways. This identification should be supported by design drawings and room walkdowns for verification. A three dimensional model could also be used for verification and validation purposes. | COM  OR | Each area of the plant containing safety-related systems or equipment is reviewed to determine the postulated fluid system failures which would result in the most adverse internal flooding conditions. For the internal flooding analysis, the failure of safety-related systems, structures or components is acceptable provided they have no safe shutdown function or the safe shutdown function is otherwise accomplished. The internal flooding analysis shows that systems, structures, and components are not prevented from performing their required safe shutdown functions due to the effects of the postulated failure. In addition, the analysis identifies the protection features that mitigate the consequences of flooding in an area that contains safety-related equipment.  See DCD [2] Section 3.4.1.2.2. The safety-related systems and components available for safe shutdown are described in DCD [2] Section 7.4.  The Owner shall be responsible for verifying hazards during plant operation. |
| 4.150. | For all possible flood scenarios, the water level as a function of time should be determined, not only for the room or plant area containing the source of the water but also for all rooms or plant areas to which the water could spread. This should take into account the overall source inventory, discharge rates and means of isolation. Possible inexhaustible water supplies should also be considered. Typical pathways that flood water could traverse include pipe conduits, drains or openings in walls or floors, stairwells, vents and elevators. Doors are also an important flood propagation pathway. | COM | The internal flooding analysis is performed based on the criteria and assumptions provided in DCD [2] Section 3.6 and ANS-56.11 [6]. The analysis consists of the following steps:   * Identification of the flood sources * Identification of essential equipment in area * Determination of flowrates and flood levels * Evaluation of effects on essential equipment   Evaluation of internal flooding has been described in the AP1000 DCD [2] in Section 3.4.1.2.2. |
| 4.151. | Flood water might travel under doors or might damage (e.g. buckle) doors until they fail, if they are not designed to withstand the hydrostatic pressure and/or hydrodynamic loads that might occur. Failure of doors should be modelled in a conservative manner.13  **\_\_\_\_\_\_\_\_\_\_**  13 ‘Conservative’ depends on whether failure of the door would be advantageous (e.g. by allowing water to flow away from SSCs important to safety) or disadvantageous (e.g. by allowing water to flow towards SSCs important to safety). | CWO | The AP1000 plant design minimizes the number of penetrations through enclosure or barrier walls below the flood level. Those few penetrations through flood protection walls that are below the maximum flood level are watertight. Any process piping penetrating below the maximum flood level either is embedded in the wall or floor or is welded to a steel sleeve embedded in the wall or floor. There are no watertight doors in the AP1000 plant design used for internal flood protection because, as described in DCD [2] Section 3.4.1.2.2, they are not needed to protect safe shutdown components from the effects of internal flooding. The walls, floors, and penetrations are designed to withstand the maximum anticipated hydrodynamic loads associated with a pipe failure as described in DCD [2] Section 3.6. The two watertight doors on the waste holdup tank compartments limit the consequence of a failure on spent fuel pool water level. |
| 4.152. | Operating experience has shown that ventilation ducts can drain water to lower levels. Thus, the propagation of water by ventilation ducts should be considered in the design. Examples of effects include water spray on electrical equipment or the submerging of equipment in rooms where there is a ventilation outlet or a low point that might fail. | COM | The analysis of potential flooding events is performed on a floor-by-floor and room-by-room basis depending upon the relative location of safety-related equipment. The analysis considers spread of water through ventilation ducts. See Section 3.4.1.2.2 in the DCD [2]. |
| 4.153. | In the case of breaks in pipes connected to tanks or pools, siphoning effects, which can increase the amount of water drained, should be considered. | COM | AP1000 plant design complies with the requirement. See DCD [2] Section 3.4.1.2.2 for details. |
| 4.154. | Possible blocking of drain holes by debris should be taken into account if this would lead to more severe conditions. In determining the water level using a volume–height relationship, the as‑built status of the room (including the volume of equipment in the room) should be used. | COM  OR | The analysis considers the effects of blocked drains. See Section 3.4.1.2.2 in the DCD [2].  The Owner shall be responsible for the as-built inspections. |
| 4.155. | If the liquid is water, flooding is usually considered to be of concern mainly for electrical devices, which should be assumed to fail if submerged or subjected to spray, unless qualified for these conditions. Cables are generally assumed to be unaffected by being submerged; however, the connection points (e.g. splices) should be assumed to fail when exposed to water unless they are specially qualified. | COM | See Section 3.11 in the DCD [2] – Environmental Qualification of Mechanical and Electrical Equipment. |
| 4.156. | Some mechanical equipment might be resistant to the direct effects of water, but rely on electrical support equipment (e.g. for power, instrumentation, control). In such cases, the effects of flooding on this support equipment should be considered. Additionally, the effect of buoyancy should be considered since mechanical equipment might not be designed to withstand an upward force. | COM | Active mechanical equipment is qualified for operability via an Operability Programme which, combined with qualification of electrical attachments, demonstrates qualification under postulated environmental conditions (including flood). Qualification of mechanical equipment for structural integrity is according to ASME Code guidelines as identified in the DCD [2] Section 3.1. |
| **PREVENTION OF INTERNAL FLOODING HAZARDS** | | | |
| 4.157. | Flooding can be caused by the leaking or breaking of a vessel, tank or pipe; therefore, design provisions intended to reduce the likelihood of a pipe leak or break (see paras 4.136–4.138) should be used to reduce the likelihood of flooding. | COM | Design measures have been taken to ensure that the probability of postulated internal flooding is minimized. Protection from internal flooding has been described in the AP1000 DCD [2] in Section 3.4.1.1.2. |
| 4.158. | The reduction of human error should be taken into account as an important way of reducing the likelihood of flooding. | COM  OR | Human factors have been considered in DCD [2] Chapter 15 and Chapter 18.  The Owner shall be responsible for implementing appropriate administrative procedures that minimize the likelihood of human error. |
| 4.159. | Engineered features (e.g. sensors) that prevent the overfilling of tanks should be used, where practicable, to limit the likelihood of internal flooding caused by tank overflow. | COM | Provisions are made to control spills of liquids due to tank overflows. For example, DCD [2] Table 11.2-3 lists the provisions for tank level indication, alarms, and overflow disposition for liquid radwaste system tanks outside containment. |
| 4.160. | Cable trays should be designed in a manner that limits flood propagation. Examples of design features to do so include drainage holes and watertight penetrations. | COM | Electrical cable (including fiber optic cable) and methods of raceway construction are selected in accordance with BTP CMEB 9.5-1 [5]. |
| 4.161. | To the extent practicable, watertight penetrations should be manufactured from material that is resistant to material degradation, and should be installed in locations that facilitate inspection and maintenance. | COM | The AP1000 plant design minimizes the number of penetrations through enclosure or barrier walls below the flood level. Those few penetrations through flood protection walls that are below the maximum flood level are watertight. They are made of degradation-resistant materials and are located in places that allow inspections. See Section 3.4.1.1.2 in the DCD [2]. |
| 4.162. | Seals and gaskets whose failure could lead to a flooding event (e.g. condenser seals) should be fabricated from a material that is resistant to material degradation and is robust enough to withstand anticipated loads (e.g. water hammer, seismic events, fire, hydraulic loads). The flow rate from a seal or gasket failure should be conservatively determined on a case by case basis. | COM | Standard engineering practice. Seals and gaskets will be fabricated using high-quality materials. The waterproofing and sealing features are described in DCD [2] Sections 3.4, 3.8 and Appendix 3D.  Where age-sensitive materials, such as gaskets and packing, are used in the assembly of mechanical equipment, the aging of these materials is normally evaluated based on an item-by-item review of the aging characteristics of the material. (See Section 3D.6.2.3).  Typical gaskets have been tested for severe accident conditions as described in NUREG/CR-5096 [23]. The gaskets for the AP1000 plant will be similar to those tested with material such as Presray EPDM E 603. |
| 4.163. | The operation of design features such as containment spray systems, fire extinguishing systems or (if in‑vessel melt retention is credited) reactor cavity flooding systems could produce flooding. Such flooding should be given full consideration in the design (e.g. some components of instrumentation and control systems should be accordingly qualified for containment sprays, and some doors and walls should be qualified as waterproof for fire extinguishing sprays). Such intentional flooding might not generally be considered an internal hazard; however, owing to its similar nature, it should be included in the set of internal flooding hazards being analysed. | COM | Protection from internal flooding has been described in the AP1000 DCD [2] in Section 3.4.1.1.2. Evaluation of internal flooding has been described in the AP1000 DCD [2] in Section 3.4.1.2. |
| **MITIGATION OF INTERNAL FLOODING AND THE EFFECTS OF INTERNAL FLOODING** | | | |
| 4.164. | Mitigation of internal flooding should be achieved in part by design choices with respect to the layout of the plant. This includes physical separation of redundant SSCs important to safety, and locating SSCs vulnerable to flooding at elevations higher than the assumed flood levels. For example, SSCs can be located on a pedestal that is higher than the maximum assumed flooding level. If this is not possible, a barrier (either a wall around the component or a complete enclosure) can be used. It should also be ensured (by all available means) that accidental flooding is mitigated as soon as possible, and that the unfavourable spreading of flooding to other areas is prevented (e.g. by means of suitable thresholds). Means that can be used to mitigate flooding include the following:  (a) Appropriate design (e.g. passive flood protection features, isolation valves on drains, pumps and watertight doors, and on potentially hazardous pipes);  (b) Detection systems (e.g. flood alarms);  (c) Adequate procedures (operational and/or emergency procedures). | COM  OR | The AP1000 plant has been designed such that flooding events within the design basis will not compromise the ability of the plant to safely shutdown. The safety functions required for safe shutdown following flooding and the supporting post 72 hour functions are shown to be maintained through a combination of provisions made on compartment barriers and the segregation of safety-related SSCs. The AP1000 plant arrangement provides physical separation of redundant safety-related components and systems from each other and from nonsafety-related components. As a result, component failures resulting from internal flooding do not prevent safe shutdown of the plant or prevent mitigation of the flooding event.  The Owner shall be responsible to implement appropriate procedures related to flood mitigation. |
| 4.165. | If actions by plant personnel are assumed (e.g. isolation of the source of flooding), the time needed to detect, diagnose and mitigate the consequences of the event should be determined. The environmental conditions in areas where actions are necessary should be evaluated and factored into any assumptions about timing. These considerations should also be factored in when determining human error probabilities. In the deterministic approach, the most limiting single failure should be assumed for detection, diagnosis or mitigatory action (e.g. isolation), and conservative times for plant personnel to complete these actions should be assumed, considering the environmental conditions due to flooding. | COM  OR | Human factors are described in DCD [2] Chapter 15 and Chapter 18. 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:   * Normal operating procedures * Abnormal operating procedures * Emergency operating procedures * Severe accident management guidelines   The Owner shall be responsible for other plant procedures and training of the personnel. |
| 4.166. | Because some means of flood detection (e.g. sump level) do not offer an indication of the precise location of the leak or break, design features should be implemented to assist plant personnel in identifying the source of internal flooding and/or to automatically mitigate the flooding. Examples include valves that automatically close if environmental conditions indicative of a flood are detected (e.g. elevated room temperature, excessive flow rate), and closed circuit television to allow visual monitoring of flooding conditions. Appropriate procedures and training should be provided for plant personnel. | COM  OR | The plant’s design to protect against internally flooding is described in detail in DCD [2] Section 3.4.1. The protection mechanisms related to minimizing the consequences of internal flooding include the following:   * Structural enclosures * Structural barriers * Curbs and elevated thresholds * Leak detection systems * Drain systems   Protection mechanisms are described in Section 3.6 in the DCD [2]. Leak detection is discussed in the AP1000 plant DCD [2] Appendix 3B.  The Owner shall be responsible for the plant procedures and training of the personnel. |
| 4.167. | The possible formation and effects of internal flood waves should be taken into account and analysed, if flooding is fast enough (such as in the event of a total breach of a large tank). A wave could increase the local water level significantly above the estimated steady state water level and therefore, a dynamic analysis should be performed. This analysis should evaluate the mechanical loads imposed on SSCs by waves and the potential effects of floating debris on SSCs. | COM | Flooding as an internal hazard has been addressed in the AP1000 plant design as described in DCD [2] Sections 3.4 and 19.56. See also the hydrodynamic analyses described in DCD [2] Section 3.8.3.4.2. |
| 4.168. | Drains are an important protective feature against flooding because they limit the rate at which water rises during a flood, which provides time for the plant personnel to take appropriate actions. The drain system should be designed with a capacity (i.e. drainage rate) suitable for the internal flooding sources in each plant area. To the extent practicable, the drainage system should be designed in a manner that facilitates inspection and maintenance to limit the likelihood of clogging. Portions of redundant drainage should be independent and not drain into common headers. Administrative controls should be used to ensure that temporary equipment that could clog drains (e.g. plastic sheeting) is not stored in a location in which it could be transported to drains if a flood were to occur. Design provisions (e.g. drains equipped with check valves) should be used to ensure that flood water from one area does not flow backwards causing a flood in another area, thus compromising the segregation of SSCs important to safety. | COM  OR | The plant’s design to protect against internally flooding is described in detail in DCD [2] Section 3.4.1. The protection mechanisms related to minimizing the consequences of internal flooding include the following:   * Structural enclosures * Structural barriers * Curbs and elevated thresholds * Leak detection systems * Drain systems   Radioactive Waste Drain System (WRS) and Waste Water System (WWS) drains are provided. WRS have been described in DCD [2] Section 9.3.5. WWS have been described in DCD [2] Chapter 3. Protection mechanisms are described in Section 3.6 in the DCD [2].  The Owner shall be responsible for the plant procedures. |
| **SPECIFIC FLOODING HAZARD CONSIDERATIONS** | | | |
| 4.169. | In addition to the direct impacts of flooding (e.g. spray, submergence) as described in this subsection, the release of water into a room might also have a significant effect on the general environmental conditions. Such effects (e.g. increase in humidity, radiation levels, temperature) should be considered in the qualification process for equipment. Special consideration should be given to potential releases of dissolved hydrogen in water and to fluids other than water (e.g. chemicals used for fire suppression). | COM | Section 3.11 in the DCD [2] discusses the qualification of the equipment required to function in the adverse environmental conditions including temperature, humidity, pressure, and chemical consequences. |
| 4.170. | The design should take into account that water present during an internal flood could impose a hydrostatic load on those SSCs in contact with the water (e.g. doors, walls, floors, penetrations). If not properly accounted for, this could lead to structural failures and damage from falling objects or heavy load drop. It could also lead to failure of barriers and doors important to safety. | COM | SSCs within the AP1000 plant have been categorized and classified in accordance with the “Categorization and Classification Methodology”. This process, which also includes fluid retaining structures, ensures that the quality requirements placed on SSCs, in terms of their design, manufacture, testing and operation, reflect their importance to safety and hence minimizes, so far as is reasonably practicable, the likelihood that they may fail to provide their safety function. Section 3.8 of the DCD [2] details the relevant design standards (primarily ASME Code, Section III), including the loading and loading combinations for the containment and associated penetrations, which includes loads from postulated pipe breaks, jet impingement, missile impact, pressure, and temperature loads. |
| 4.171. | The design of the plant should ensure that potentially contaminated water released during a flooding event does not propagate into the site surface and/or groundwater. One method of achieving this is to ensure that those portions of the building that are below the assumed maximum flood level are leaktight. | COM  OR | Water within containment and the radiologically controlled area of the auxiliary building will ultimately be discharged through the liquid radwaste system (WLS). Water within the other buildings will be discharged through the waste water system. The sumps allow for sampling and the discharges are monitored. The Owner shall be responsible for ensuring that water drainage from areas that may contain radioactivity are collected, sampled, and analyzed before discharge to the environment. |
| 4.172. | Leakages from systems used in the long term for extracting heat from the containment during severe accidents should be accounted for. These systems should be capable of being isolated, and any radioactive water and gas released should be confined by appropriate means; in particular, a ventilation system qualified to the corresponding ambient conditions should be available. | COM | The PCCWST (Passive Containment Cooling Water Storage Tank) is not considered to be a credible source of internal flooding in containment, as this water is located outside of the containment vessel and any water that runs off the containment outside surface goes to drains in the shield building annulus.  The containment and penetration design includes features specifically designed to minimize overall containment leakage. See DCD [2] Section 6.2.3 for additional details. |
| **HEAVY LOAD DROP** | | | |
| 4.173. | The collapse of structures, or objects falling from heights, can be secondary effects either of an internal hazard or of an external hazard such as an earthquake or high winds. They need to be assessed as potential consequences of the initiating internal or external hazards. In turn, falling objects can cause consequent internal hazards; guidance on these combined sequential hazards is given in Appendix I. Paragraphs 4.174–4.186 concentrate on heavy load drop in which no other initiating hazard is necessary. | COM | Prevention measures against load drops are discussed in DCD [2] Chapter 9. |
| **IDENTIFICATION AND CHARACTERIZATION OF HEAVY LOAD DROP** | | | |
| 4.174. | Drops are most likely to occur during the handling of plant equipment for maintenance or during fuel handling lifts. If heavy items of plant equipment are located at significant heights, an evaluation should be made of the possible hazards associated with dropping such equipment, unless the probability of such an event is negligible. The consequences of heavy load drops should be assessed as these consequences could present a risk to safety in several ways, including the following:  (a) As an impact on the fuel (risk of radioactive release and potentially risk of criticality);  (b) As an impact on components of safety systems (risk of failure of systems);  (c) As an impact on structures important to safety (e.g. risk of loss of integrity of fuel pools and of release of radioactive material). | COM | The AP1000 plant handling systems are described in the DCD [2] Sections 9.1.4 and 9.1.5. A dropped load is deterministically assumed to occur as a result of a failure of a lifting device. The consequences of heavy load drops have been assessed. |
| 4.175. | IAEA Safety Standards Series No. SSG‑62, Design of Auxiliary Systems and Supporting Systems for Nuclear Power Plants [12], and IAEA Safety Standards Series No. SSG‑63, Design of Fuel Handling and Storage Systems for Nuclear Power Plants [13] provide recommendations on the design of overhead lifting equipment and fuel handling equipment respectively. Furthermore, IAEA Safety Standards Series No. SSG‑67, Seismic Design for Nuclear Installations [14], and IAEA Safety Standards Series No. SSG‑74, Maintenance, Testing, Surveillance and Inspection in Nuclear Power Plants [15], provide recommendations on seismic design and qualification, and on maintenance, surveillance and in‑service inspection, respectively, that together will lead to high integrity lifting systems in operation. Following the recommendations of these publications will reduce the likelihood of dropping heavy equipment as a result of internally initiated events. | NR | This is a statement not a requirement. |
| 4.176. | The nature of the object and the cause of the drop should be analysed in order to characterize the possible direction (e.g.from drop, tilting or swinging), size, shape and energy of the falling object and the possible consequences for safety.14  **\_\_\_\_\_\_\_\_\_\_**  14 The following cases are assessed in some States with realistic assumptions: drop of the reactor pressure vessel closure head on the reactor pressure vessel, drop of the reactor cavity cover slab on the reactor pressure vessel closure head (when the slabs above the vessel are removed) and drop of the reactor cavity cover slab on the reactor cavity floor slab. | COM | The AP1000 plant handling systems are described in the DCD [2] Sections 9.1.4 and 9.1.5. A dropped load is deterministically assumed to occur as a result of a failure of a lifting device. The arrangement of the system in relationship to safety-related plant components is such that the consequences of a load drop are acceptable per NUREG 0612. Postulated load drops are evaluated in the heavy loads analysis.  A dropped load onto the reactor vessel can only happen in Plant Operation Modes 5 and 6, when Containment is open and the lifting equipment within it is used to support refuelling operations. The bounding load that could be dropped onto the reactor vessel is the IHP. Analysis has been conducted that demonstrates that the reactor pressure vessel and associated supports and connections will withstand the impact from the dropped load. |
| 4.177. | For the purpose of determining the potential consequences, dropped loads associated with fuel handling could be considered in categories such as casks or lids, transfer casks and multipurpose sealed baskets or canisters, fuel and fuel storage racks, and power and hand operated tools. Fuel handling drops constitute a large variety of different scenarios, and each needs to be considered in the context of the potential radiological consequences and the potential effect on SSCs. | COM | 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. Plant arrangement and the design of heavy load handling systems are based on the following criteria:   * To the extent practicable, heavy loads are not carried over or near safety-related components, including irradiated fuel and safe shutdown components. Safe load paths are designated for heavy load handling in safety-related areas. * The likelihood of a load drop is extremely small (that is, the handling system is single failure proof), or the consequences of a postulated load drop are within acceptable limits.   Measures and procedures are in place to avoid that unintentional dropping of loads that could affect items important to safety. Quantification of the consequences of a dropped load is given in the DCD [2] Chapter 9. |
| 4.178. | Another potential category of dropped loads is associated with the movement of containers for radioactive waste. In general, these are likely to contain materials with lower activity levels than fuel casks, but the containers are also less substantial. The general principles of prevention of drops and limiting consequence should also be followed when handling containers for radioactive waste (i.e. in the quality of lifting equipment, the choice of routes and controls to prevent incorrect operation). | COM  OR | As presented in DCD [2] Section 11.4.1.3, waste disposal containers are to be selected from available designs that meet the requirements. Packaged solid radwaste is stored in the radwaste building. This material is bagged or loaded into storage containers at the point where it is generated/processed. All LLW (Low Level Waste) will have been pre-packaged and this may include some encapsulated waste. The LLW processing equipment for dispatch to LLWR is expected to be permanently installed. Given that these containers are typically stainless steel, a dropped load is unlikely to result in container breach.  The Owner shall be responsible for procedures and controls of the handling systems. |
| **PREVENTION OF HEAVY LOAD DROP** | | | |
| 4.179. | Functional design requirements often govern the physical location of equipment in this category. Where it is functionally necessary to tolerate proximity between heavy equipment and targets, it is possible to provide sufficient design measures such as redundant cables on cranes or interlocks to reduce the probability of failure. Guidance on the design of high integrity and single failure proof cranes is available in Refs [16–19]. | NR | This is a statement not a requirement. |
| 4.180. | Where practicable, plant layout should facilitate the safe movement of the overhead lifting equipment and of items being transported. In some cases, it might be necessary to handle plant equipment in areas where the layout precludes separation from SSCs important to safety; in such cases, additional care should be taken in the handling of heavy loads in the vicinity of SSCs. | COM | The consequences of dropped loads are minimized by ensuring that loads that have to be lifted above SSCs delivering safety-related functions are moved:   * At the minimum height compatible with safely completing the move. * Have safe load paths specified. * Have physical stops to prevent the hook from travelling over or near SSCs. * Have procedural controls linked to plant operating mode to reduce the consequences of a dropped load. (The cranes that are operated within the containment building can only be operated when the reactor plant is in either mode 5, cold shutdown or mode 6, refueling. In both cases the RCS is below 200°F (93°C) and its operating pressure is very low or at atmospheric pressure.) |
| 4.181. | Measures to prevent dropped loads should include the classification of lifting devices, design measures and administrative measures, as follows:  (a) Classification of lifting devices in accordance with the results of a hazard analysis that evaluates the consequences of a postulated dropped load.  (b) Design measures:  (i) The general considerations of the first level of defence in depth, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation.  (ii) Crane zoning and protection schemes, as appropriate, including load cells to monitor lift weights, and interlocks and trips.  (c) Administrative measures:  (i) Procedural controls to prevent the lifting of excessive loads, or the inadvertent mishandling of loads (e.g. load snagging, load hold‑up, swinging loads).  (ii) Appropriate controls related to the identification of appropriate lift heights and lift routes, and administrative controls to enforce these (e.g. additional supervision). There could also be advantages in local control of a lift such that plant personnel can confirm that there are no snags or hold‑ups and that clearances are adequate for the lift.  (iii) Periodic inspection and maintenance of cranes (e.g. their interlocks, cables and brakes) and associated lifting equipment (nooses and slings, straps and shackles, and related items). | COM  OR  POS | a) The classification of lifting devices is discussed in the DCD [2] Sections 9.1.4 and 9.1.5. Table 3.2-3 in DCD [2] provides classification of fuel handling components and equipment.  b) The risk from a dropped load has been reduced to levels which are ALARP through application of best practice to the design and operation of the lifting devices, together with procedural controls. Monitoring and protection devices to mitigate the risk of a dropped load, overload or crane collapse are provided.  c) The Owner shall be responsible for procedures, controls, and inspections of the handling systems. |
| 4.182. | Prevention of dropped loads in fuel handling is mostly achieved through conservative design measures and appropriate administrative measures. Fuel handling layout and lift routes should be designed to avoid potential drops on SSCs important to safety. | COM  OR | The design and arrangement of heavy load handling systems promotes the safe handling of heavy loads by one of the following means:   * A single-failure-proof system is provided so that a load drop is unlikely. * The arrangement of the system in relationship to safety-related plant components is such that the consequences of a load drop are acceptable per NUREG 0612. Postulated load drops are evaluated in the heavy loads analysis.   The fuel handling machine performs fuel handling operations in the new and spent fuel handling area. It also provides a means of tool support and operator access for long tools used in various services and handling functions. The fuel handling machine is equipped with two 2-ton hoists, one of which is single failure proof and is designed according to NUREG-0554.  The cranes and lifting equipment to be used within the NI have been identified, together with the SSCs delivering safety functions that could be impacted by a dropped load from this equipment. For some crane lifts, it can be shown that a dropped load will not impact SSCs delivering safety functions. Where SSCs delivering safety functions can be impacted it is shown for the majority of lifts that other SSCs will continue to provide the safety functions. |
| 4.183. | A design objective for the plant layout should be to protect stored fuel or other items important to safety from the drop of heavy equipment or other equipment handled in specific situations that might induce serious consequences. | COM | Plant arrangement and the design of heavy load handling systems are based on the following criteria:   * To the extent practicable, heavy loads are not carried over or near safety-related components, including irradiated fuel and safe shutdown components. Safe load paths are designated for heavy load handling in safety-related areas. * The likelihood of a load drop is extremely small (that is, the handling system is single failure proof), or the consequences of a postulated load drop are within acceptable limits. * Single-failure-proof systems can stop and hold a critical load following the credible failure of a single component. * Single-failure-proof systems can support a critical load during and after a safe shutdown earthquake.   See Sections 9.1.4 and 9.1.5 in the AP1000 plant DCD [2]. |
| **MITIGATION OF THE EFFECTS OF HEAVY LOAD DROP** | | | |
| 4.184. | A significant mitigation of risks from dropped loads is provided by scheduling load movements and lifts only in specified modes of plant operation (such as shutdown modes). Such scheduling could be also used as a preventive measure. | NR | This is a statement not a requirement. |
| 4.185. | The consequences of heavy load drops can in some cases be reduced by adopting a stepped approach so that the lift is made over intermediate points, by using load following platforms or by deploying deformable structures at the point of the lift. Protective dampers could also be installed on heavy loads. For example, such protective dampers are used for fuel casks. | NR | This is a statement not a requirement. |
| 4.186. | For crane loads associated with fuel handling, such as fuel shipping casks, particular attention should be paid to the fuel casks because of their large mass. The possible consequences of drops affecting the fuel storage pool should be controlled. Impacts of concern might include a fall either into the fuel storage pool or onto the slabs surrounding the pool. These impacts should be assessed as potentially compromising the integrity or leaktightness of the storage pool. Another layout practice that should be considered is to restrict the handling of fuel casks to an area remote from the pool itself and remote from other target areas (see SSG‑63 [13]). | COM | The cask crane is designed so that it cannot access the new or spent fuel pits. This is performed with hard stops to physically limit the access of the crane.  The facility is designed so that heavy objects, such as the spent fuel shipping cask, cannot be carried over or tipped into the spent fuel pool, thus only dropping of a fuel assembly as the most conservative scenario is taken into consideration.  For more information see APP-GW-G0R-013 [24]. |
| **ELECTROMAGNETIC INTERFERENCE** | | | |
| 4.187. | Electromagnetic interference is a term used to describe a number of potential disturbance mechanisms with the potential to affect electrical or electronic devices caused either by electromagnetic conduction or by electromagnetic radiation. If the disturbance is in the high or radio frequency ranges, it is sometimes referred to as radio frequency interference; in the context of this Safety Guide, electromagnetic interference is used as the generic term. | NR | This is a statement not a requirement. |
| 4.188. | Electromagnetic interference hazards can be categorized as internal hazards (e.g. caused by induction or radiation from installed equipment, either in normal operation or in fault) or as external hazards (e.g. lightning, radiation from solar flares, or radiation from equipment outside the site boundary and operated by other bodies). This Safety Guide addresses internal electromagnetic interference hazards only. | NR | This is a statement not a requirement. |
| 4.189. | In many cases, both prevention of the sources of electromagnetic interference and the ability of equipment to withstand electromagnetic interference are addressed by the standards for design and construction of equipment. Further recommendations on these aspects are provided in SSG‑39 [6] and SSG‑34 [7]. | NR | This is a statement not a requirement. |
| **IDENTIFICATION AND CHARACTERIZATION OF ELECTROMAGNETIC INTERFERENCE HAZARDS** | | | |
| 4.190. | The potential sources of electromagnetic interference should be identified and possible effects from them should be assessed. Significant sources of electromagnetic interference within the control of the operating organization include motor and generator brush assemblies, and fault current clearance from the operation of switchgears, circuit breakers or fuses. Electric fields can also be caused by radio transmitters. Even flash photography has occasionally affected sensitive control and protection equipment. There is considerable operating experience feedback available that will help designers identify potential electromagnetic interference mechanisms or similar faults. Further recommendations are provided in SSG‑39 [6]. | COM | The AP1000 plant takes two complementary approaches to the control of the hazard from EMI. These are the protection of systems from EMI (i.e. susceptibility), and the minimization of EMI at source (i.e. emissions).  To ensure that the I&C systems operate correctly in the presence of EMI, the AP1000 plant adheres to standards and follows best practice in the characterization of the electromagnetic environment, the design of the systems, the selection of system components, the placing of the systems equipment and the testing of the systems when installed. This philosophy for the management of electromagnetic compatibility for the AP1000 plant design is set out in Appendix 3D of the AP1000 DCD [2]. See also DCD [2] Chapter 7 and DCD Chapter 8 (“Electrical disturbances and electromagnetic interferences”). |
| 4.191. | Other potential sources of electromagnetic interference include some maintenance or construction activities, for example portable arc welding equipment and portable radio communications equipment brought into the nuclear plant, and ground penetrating radar used for ground surveys. These potential sources of electromagnetic interference should also be identified and possible effects from these sources should be considered. | COM | See DCD [2] Chapter 7 and DCD Chapter 8 (“Electrical disturbances and electromagnetic interferences”). Philosophy for the management of electromagnetic compatibility for the AP1000 plant design is set out in Appendix 3D of the AP1000 DCD [2].  All credible sources of electromagnetic interference have been considered in the AP1000 plant design. |
| 4.192. | Identification of potential electromagnetic interference hazards should take into account potential sources arising from faults, for example electrical faults from cables with insulation degradation or transformer bushing insulator breakdown faults. | COM | See DCD [2] Chapter 7 and DCD Chapter 8 (Electrical disturbances and electromagnetic interferences). Philosophy for the management of electromagnetic compatibility for the AP1000 plant design is set out in Appendix 3D of the AP1000 DCD [2]. |
| 4.193. | The identification process should, where possible, also include the location of sources of electromagnetic interference. This will be relevant when assessing the effects of the interference on the plant. | COM | All likely generators of EMI within the AP1000 plant have been identified. Electrical equipment can generate EMI by conduction through cables, radiated magnetic fields, radiated electric fields, or ESD. Likely generators of EMI have been specified to minimize the risk of them spuriously generating levels of EMI that could cause a hazard to AP1000 plant equipment, including safety-related equipment. |
| **PREVENTION OF ELECTROMAGNETIC INTERFERENCE HAZARDS** | | | |
| 4.194. | The nuclear power plant design should include preventive and/or protective measures against the effects of electromagnetic interference. An assessment should be made to determine whether any source of electromagnetic interference on the site could cause malfunction in, or damage to, the nuclear power plant’s systems and components, particularly instrumentation. During the plant’s operating lifetime, both the presence of new sources of electromagnetic interference and changes in existing sources should be monitored and analysed. | COM  OR | The AP1000 plant design addresses EMI for safety-related equipment in a manner consistent with the US NRC recommendations in Regulatory Guide 1.180 (“Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems”) in the licensed country of origin. The AP1000 plant design applies a standard method of placing electronics equipment in properly constructed metal cabinets/enclosures that shield enclosed equipment from the surrounding electromagnetic fields.  The Owner shall be responsible for procedures, controls, and inspections. |
| 4.195. | Electromagnetic interference should be limited such that the functioning of equipment is ensured. Recommendations on minimizing the effects of electromagnetic interference on instrumentation and control components or systems are provided in SSG‑39 [6]. This includes a number of techniques, such as the following:  (a) Suppression of electromagnetic noise at the source;  (b) Separation and isolation of instrumentation and control signal cables from power cables;  (c) Shielding of equipment and cables from external sources of magnetic and electromagnetic radiation;  (d) Filtering of electromagnetic noise before it can couple to sensitive electronic circuits;  (e) Neutralization or isolation of electronic equipment from ground potential differences;  (f) Proper grounding of electrical and instrumentation and control equipment, raceways, cabinets, components and cable shields.  Adoption of these techniques can ensure a good level of compatibility between instrumentation and control systems and the sources of electromagnetic interference in the local environment. | COM | The AP1000 plant design applies a standard method of placing electronics equipment in properly constructed metal cabinets/enclosures that shield enclosed equipment from the surrounding electromagnetic fields. Electrical equipment is suitably specified, rated and with sufficient system protection to ensure that electrical faults are minimized by design. See also responses to Sections/Paragraphs 4.194 and 4.199.  See also APP-GW-G0R-007 [30]. |
| 4.196. | If testing is to be carried out to demonstrate the effectiveness of the protection against electromagnetic interference provided by the design, the equipment under test should be in a state such that if it were to operate incorrectly this would not adversely affect safety. The tests should be performed using typical operating parameters (e.g. input signal, output signal, ambient conditions, auxiliary power supply, electrical characteristics). | COM  OR | EMC tests will be performed using typical operating parameters.  The Owner shall be responsible to meet this requirement during the post-installation tests. |
| 4.197. | Portable sources close to sensitive equipment should be controlled in such a way that SSCs important to safety will not be adversely affected by these sources. This could include a number of measures, such as exclusion zones15 or other administrative controls. Exclusion zones should be reinforced by physical controls (e.g. electromagnetic interference detection devices), by administrative controls (e.g. access arrangements, warning notices, work control systems) and by good safety culture (training, awareness, self‑checking, questioning attitude). The choice of approaches to enforce exclusion zones will depend upon the level of reliability that is needed.  **\_\_\_\_\_\_\_\_\_\_**  15 An exclusion zone is defined by the minimum distance permitted between the point of installation of an SSC important to safety and where portable sources of electromagnetic radiation are allowed to be activated. | OR | Appropriate administrative controls (e.g. exclusion zones) shall be provided by the Owner. |
| 4.198. | The consequences of individual component failures on the overall performance of systems or on the overall safety function should be understood. | COM | The consequences of individual component failure are considered in the AP1000 plant design. |
| 4.199. | As with other internal hazards, good design principles such as redundancy and diversity, and physical separation and segregation should be adopted as they can significantly reduce the pervasiveness of the electromagnetic interference hazard. In many cases, care in the design regarding the location of systems or subsystems can have a major effect on the potential overall consequences to system functionality and hence to the performance of safety functions. | COM | The distribution of safety-significant SSCs on an AP1000 plant is such that complete loss of operability of the safety-significant SSCs within a room or compartment because of EMI would not result in the loss of a safety function.  Adequate redundancy is provided within each safety-related system such that even if the loss of a single SSC were to occur, the safety function can still be provided by a redundant train located in a different compartment or area of the containment building. This compartmentalization of safety systems provides some protection from system disruption due to EMI. It is recognized that the form of the physical barriers and the separation while adequate for physical hazards such as fire are flood may not be completely adequate for EMI which can propagate widely. However, the physical barriers and the redundancy separation and segregation of system do provide some protection to AP1000 plant systems by the creation of Faraday cages.  Each of the four divisions of the protection and safety monitoring is completely segregated from the others, so any on-site EMI would have to affect more than one division before any nuclear safety consequences could occur. The complete loss of operability of electronic equipment within a cabinet would not result in a challenge to a safety function. |
| **SPECIFIC ELECTROMAGNETIC INTERFERENCE HAZARD CONSIDERATIONS** | | | |
| 4.200. | This Safety Guide considers only the ‘prompt’ effects of electromagnetic interference as an internal hazard. It is possible that standing electromagnetic interference has long term effects, in terms of induced vibrations and fatigue or galvanic corrosion through eddy current effects. These might have an effect on long term integrity of components and systems, but it is assumed that these would be managed by processes intended to maintain the condition of the plant. | NR | This is a statement not a requirement. |
| **RELEASE OF HAZARDOUS SUBSTANCES INSIDE THE PLANT** | | | |
| 4.201. | Hazardous substances have the potential to disable plant items or systems or to affect personnel carrying out actions important to safety. The potential to release stored hazardous substances or to generate them within the site boundaries is considered as an internal hazard within this Safety Guide. The release of hazardous material from outside the site or outside the control of the operating organization should be considered as an external hazard (e.g. chlorine release from road tanker accident). However, some of the recommendations in this Safety Guide could also be relevant in such design considerations. | COM | Release of hazardous substances is described in DCD [2] Section 2.2 and Chapter 11. |
| 4.202. | The effects of hazardous chemical substances that should be considered in the safety analysis should include the effects due to physicochemical properties (e.g. explosive, oxidizing, flammable) and health threatening properties (e.g. toxic, irritant, corrosive, anoxic, high temperature). | COM | The effects of hazardous chemical substances are considered in DCD [2] Section 2.2 and DCD Chapter 11. |
| **IDENTIFICATION AND CHARACTERIZATION OF HAZARDS FROM RELEASES OF HAZARDOUS SUBSTANCES WITHIN THE PLANT** | | | |
| 4.203. | The inventory of hazardous materials (i.e. quantity, physical and chemical form, type, storage arrangements) within the site boundary should be reviewed to determine what materials, if released, could either affect components of systems important to safety, or cause adverse effects on personnel that might affect their ability to carry out actions important to safety. | COM  POS | The AP1000 plant uses defined and limited quantities of hazardous material on site to support the operation of the plant. Table 6.4-1 of the DCD [2] lists the principal hazardous materials present on an AP1000 site and where they are stored. Other intrinsically hazardous material is present on site, but in such small quantities that it poses a minimal threat.  The precise selection of chemicals and volumes may change based on site-specific requirements and operating experience. |
| 4.204. | A list of the hazardous substances that could potentially be released should be established by a hazard identification process. These potential releases could come from a variety of differing sources, for example: bulk stored gases, bottled gases, volatile liquids, chemicals used in water chemistry, and releases of chemicals that could mix and form a secondary product, for example as a cloud. | COM  POS | See response to Section/Paragraph 4.203. |
| 4.205. | The list of hazardous substances should be complete and should include any such substances that are brought onto the site by subcontracting companies for maintenance purposes. | OR  POS | The list of hazardous substances brought onto the site by subcontracting companies shall be prepared by the Owner.  The precise selection of chemicals and volumes may change based on site-specific requirements and operating experience. |
| 4.206. | Potential effects of the hazard on plant personnel should be considered. These could include toxic and asphyxiation effects with the potential to disable or otherwise impair plant personnel. Care should be taken to ensure that the release of hazardous substances would not prevent actions by plant personnel to control the incident or to safely shut down the plant and maintain it in a safe state. | COM | The potential effects of toxic substances on personnel have been considered. Appropriate protective measures have been provided. |
| 4.207. | Potential effects of the hazard on the plant’s SSCs should also be considered. Examples include deposition causing shorting at electrical contacts for instrumentation and control equipment, and the intake of non‑combustible gases by diesel generators that might cause them to fail to run. In addition, some plant systems could be affected by the cooling effects of gas clouds. Prompt or short term potential corrosion effects should be also identified. | COM | See response to the Section 4.213. |
| **PREVENTION OF HAZARDS FROM RELEASES OF HAZARDOUS SUBSTANCES WITHIN THE PLANT** | | | |
| 4.208. | Measures to prevent releases of hazardous substances include the general considerations of the first level of defence in depth with respect to minimizing the likelihood of a release, including conservative design and material choices, high quality in construction, and surveillance both in construction and operation. Specific measures relevant to releases of hazardous substances include design of storage tanks and distribution systems, and their in‑service maintenance. | NR | This is a statement not a requirement. |
| 4.209. | Where plant systems or components need to be resilient to the presence of a gas or vapour cloud, the same approach should be followed (i.e. conservative design and material choices, high quality in construction, and surveillance both in construction and operation). In such cases, cabling and electrical control cabinets close to potential releases should be designed and located so as to minimize (consistent with other safety requirements) damage due to the release of gas, water, steam, smoke or hazardous substances. | COM  OR | The risk from a release of toxic, corrosive, and flammable materials is minimized by ensuring that:   * Bulk storage of gases and chemicals is in locations where an uncontrolled release cannot threaten safety-related SSCs. * Storage of gases and chemicals are in vessels and containers that are constructed to appropriate codes of practice and where necessary provided with secondary containment (e.g. bunds or dikes) to contain accidental spills and leaks. * Transport of material from the bulk storage location to local storage or use locations will be carried out in accordance with procedures and by processes that minimize the risk of an uncontrolled release of material. * Materials are held and used in the minimum quantities within the NI necessary for AP1000 plant operation. * Other intrinsically hazardous materials are present on site, but in such small quantities as to pose minimal threat and will be risk assessed and controlled by procedures and permits-towork.   Raceways are kept at a reasonable distance from sources of hazardous substances.  The Owner shall be responsible for procedures, controls, and inspections. |
| 4.210. | As with other internal hazards, adoption of good design principles such as redundancy and diversity, and physical separation and segregation can have a significant effect on the development of hazards from releases of hazardous substances. In some cases, scenarios of concern can be largely eliminated by carefully locating safety systems (i.e. relative to the storage arrangements for hazardous materials). | NR | This is a statement not a requirement. |
| 4.211. | Where necessary, the prevention of hazards from releases of hazardous substances should include controls for ventilation systems for plant areas where actions to fulfil safety functions are needed, in particular in control rooms. Control systems should close ventilation intakes, putting the area into a recirculation mode and thereby preventing incapacitating effects on plant personnel performing actions important to safety. Recommendations on the design of the ventilation systems are provided in SSG‑62 [12]. | COM | Site habitability is also a concern for toxic materials. The AP1000 plant has an additional level of defense against toxic airborne material. With advanced warning, the operators may actuate passive control room habitability. This system isolates the control room from normal HVAC and actuates a separate system supplied from compressed air containers. The compressed air slightly pressurizes the control room above atmospheric pressure, preventing the entrance of toxic material in the control room. This system is available for 72 hours, which is adequate time to withstand the event.  The main control room emergency habitability system provides main control room habitability in the event of a design basis accident (DBA) and is described in DCD [2] Section 6.4. |
| 4.212. | In the case of releases of chemicals that could mix and form a secondary hazardous product, the preventive measures should include administrative controls over the receipt and storage of such chemicals, and engineering provisions, for example, different hose couplings for acid and alkaline supplies. | OR | The Owner shall be responsible for administrative control over receipt and storage of chemicals. |
| **MITIGATION OF THE CONSEQUENCES OF HAZARDS ASSOCIATED WITH RELEASES OF HAZARDOUS SUBSTANCES WITHIN THE PLANT** | | | |
| 4.213. | The design principles of redundancy and diversity, and physical separation and segregation of SSCs important to safety should also mitigate the effects of hazards associated with releases of hazardous substances. Systems that include redundant capability with good segregation or separation should have sufficient redundant subsystems unaffected by the release that their safety functions will be successfully fulfilled even with failures in some of the system components. | COM | The containment structure provides a barrier to the intrusion of toxic gases into the area where the main safety-related components are sited. Outside the containment structure, the plant, and its safety-related SSCs have been designed so that the complete loss of the equipment within any single room will not result in loss of the safety function. The fire barriers protecting redundant trains of the safety-related SSCs from fire should also provide an adequate barrier to spread of corrosive liquids and toxic or flammable gases and therefore limit any damage to the equipment in one room.  DGs rely on an air supply to maintain their function. The DGs are located in the DG building which is remotely sited from the other plant buildings and is on the opposite side of the turbine building to the PGS. The DG building and motor air inlets are located close to the ground so that the heated gases from a postulated fire affecting a diesel oil storage tank will not prevent DG motor start-up or operation. In addition, the batteries providing power to the safety-related SSCs would not be susceptible to an asphyxiant gas.  Adequate redundancy is provided within each safety-related system such that even if the loss of a single SSC as a result of, for example a fire which is assumed to disable the whole train, the safety function can still be provided by a redundant train located in a different fire compartment (or fire zone within the containment building). This compartmentalization of safety systems also provides protection from system damage due to ingress of toxic or corrosive liquids. In addition, penetrations between compartments are minimized mainly to reduce the potential routes for the spread of gases.  Taking account of the potential loss of those SSCs affected by the toxic, corrosive or flammable material concurrent with a credible unrelated single failure within the other SSCs it is concluded that sufficient redundancy, diversity and segregation is provided in the design and location of the SSCs ensures that the safety functions are maintained in the worst-case, normally permitted, plant line-up. |
| 4.214. | The effects of locating the plant and equipment within buildings could mean that gas clouds have blown past or reduced in density before significant ingress into the building that might affect the local environment for equipment such as cables and cubicles. | NR | This is a statement not a requirement. |
| 4.215. | Accident management might necessitate the provision of personal protective equipment to allow plant personnel to escape from environments that are in danger of becoming uninhabitable, access plant areas in which important actions have to be carried out or continue performing other actions at an endangered location (e.g. for plant personnel in the main control room). | OR | The Owner shall be responsible for providing appropriate personal protective equipment. |
| **SPECIFIC CONSIDERATIONS FOR RELEASES OF HAZARDOUS SUBSTANCES** | | | |
| 4.216. | This Safety Guide considers only the ‘prompt effects’ of the release of hazardous material within the plant. It is possible that smaller continuing releases could cause long term effects, for example, in terms of corrosion effects. These might have an effect on long term component or system integrity, but these should be managed by processes intended to maintain the condition of the plant. | OR | This requirement shall be the responsibility of the Owner. |

## 

## 2.5. APPENDIX I – HAZARD COMBINATIONS

| **Section/Paragraph** | **Requirement**  **Note:** The references noted in [] in column “Requirement” do not relate to the reference list in Section 4.0 of this document but relate to the reference list of the IAEA Specific Safety Guide SSG-64. | **Compliance** | **Justification** |
| --- | --- | --- | --- |
| I.1. | Both internal hazards and external hazards can cause other hazards. For example, a seismic event (external hazard) could result in the rupture of a pipe or cause a fire by damaging electrical equipment (internal hazards). Similarly, the drop of a heavy load (internal hazard) might cause an internal flood (another internal hazard) by breaking a pipe or it might generate missiles (internal hazard) by damaging mechanical equipment. | NR | This is a statement not a requirement. |
| I.2. | The effects of these combined hazards (i.e. two or more hazards occurring as a consequence of an initial event, including a hazard) should be considered in the plant’s design. The combinations that should be considered depend on the location of the site and the general plant design. Combinations involving a variety of external hazards (natural hazards such as tsunami, blizzard and sandstorm, and also human induced ones such as explosion pressure waves) are not applicable to all sites. Therefore, it is not feasible or necessary to identify a set of hazard combinations that are applicable to all plants. | COM  POS | The AP1000 plant PRA [4], 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. |
| I.3. | A performance based approach16 is recommended. This approach, irrespective of the specific methods or criteria being used, should be comprehensive and systematic. The objective is to identify which hazard combinations need to be considered and which design features are necessary to address these combinations. The basis for screening a hazard combination for further consideration, as well as for screening out combinations of hazards, should be clearly defined and documented.  **\_\_\_\_\_\_\_\_\_\_**  16 A performance based approach does not prescribe specific steps that have to be taken, but rather defines a desired outcome and clear, objective, and measurable criteria to determine whether that outcome has been reached. Various methods could be used, provided the desired outcome is reached. | COM | See response to Section/Paragraph I.2. |
| I.4. | In principle, the following three types of hazard combination could be considered:  (a) Consequent (subsequent) events: An initial event (e.g. an external or internal hazard) results in another event (e.g. an internal hazard). Examples are a seismic event and subsequent internal explosion, and internal fire and subsequent internal flooding.  (b) Correlated events: Two or more events, at least one of them representing an internal hazard, which occur as a result of a common cause. The common cause can be any anticipated event, including an external hazard, or might be due to an unanticipated dependency. The two or more events connected by this common cause could occur simultaneously17. Examples include a tsunami as the common cause for external flooding, internal flooding and internal fire as three potential correlated events, and electromagnetic interference as the common cause for station blackout and internal fire as the two correlated events.  (c) Unrelated (independent) events: An initial event (e.g. an external or internal hazard) occurs independently from (but simultaneously with) an internal hazard without any common cause. Examples are external flooding and an independent internal explosion, and a seismic event and an independent internal fire.  **\_\_\_\_\_\_\_\_\_\_**  17 ‘Simultaneously’ in this case does not mean that the hazards occur exactly at the same time but rather that the second hazard occurs before the effects of the previous hazard have been completely mitigated. | NR | This is a statement not a requirement. |
| I.5. | A hazard combination sequence should be used to determine the loading and magnitude of the hazard, the duration it is applied, and the sequencing of the occurrence of other hazards. For unrelated (independent) events, an identification process should be adopted to include all foreseeable independently occurring hazards, where the second is sufficiently probable that it could occur before the effects of the previous hazard have been completely mitigated. Correlated hazards result from the same basic failure, or other common cause initiator, and the frequencies are related to the cause. Consequent hazards could occur at the same frequency as the initial hazard, or at a lower frequency, depending on the progression of events leading to the subsequent hazards. | COM | When 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, then such combinations of event are considered to be design basis events depending on the likelihood of occurrence. To this end, combinations of internal hazards within the design basis will be evaluated where:   * An internal hazard induces sequential internal hazard(s); or * A common initiator results in simultaneous internal hazards; * Independent internal hazards with a combined event frequency > 1E-05/reactor year. |
| I.6. | Hazard identification processes could produce a long list of potential combinations; therefore, pragmatic approaches should be used. While combinations involving two (or even more) simultaneous hazards could be postulated, screening criteria should be developed to ensure that the list represents a credible and reasonable set of plant challenges. The screening criteria can be deterministic or probabilistic, or a combination of both. Examples of screening criteria include the following:  (a) The event combination is not credible;  (b) The event combination, even if credible, would not lead to conditions beyond what have already been assumed in the design. | COM  POS | Where a mechanism has been identified to link two (or more) internal hazards, a room-by-room analysis has been undertaken identify locations where the two internal hazards and associated mechanism exist. Where this is the case, the combination of internal hazards has been subject to detailed assessment.  The consequences of combinations of internal hazards are based on the combined effects of the individual hazards. The effects of the individual internal hazards are taken from the respective hazard schedules. Unless one of the internal hazards causes the loss of SSC provided to prevent, protect or mitigate the internal hazard progression, the effect of each individual internal hazard is taken as the fully mitigated consequences.  The site-specific analysis will need to address the identification of the site-specific hazards. |
| I.7. | The desired outcome of this process is a clear understanding of any unique effects of hazard combinations that should be accounted for in the design of the plant. For example, in the case of internal flooding, if the maximum flood level in a room caused by a load drop or missile impact exceeds the assumed flood level caused by a pipe break, additional design measures could be necessary. On the other hand, if analysis shows that existing hazard analysis (based on pipe rupture) predicts a flood level greater than what could be caused by a missile or load drop, no additional design measures would be necessary. | COM | Deterministic links have been identified between internal hazards as follows:   * An internal fire may be initiated by internal flooding, missiles or dropped loads; * An internal flood may be initiated by internal missiles, dropped loads or pressure part failure; * An internal missile may be initiated by internal fire, flooding or dropped loads; * A dropped load may be initiated by internal missiles or pressure part failure; * An internal explosion may be initiated by internal fire, flooding, missiles, dropped loads or pressure part failure; * A pressure part failure may be initiated by internal missiles or a dropped load.   Mechanisms as possible causes for initiating internal hazards associated with onsite transport, biological fouling, toxic, corrosive, or flammable chemicals and electromagnetic interference have not been identified on the basis that these internal hazards do not result in loss or damage of safety-related SSC and as such their contribution to combinations of internal hazards is of no consequence.  The assessments covering each of the systematically-identified internal hazards conclude that the high level, prevention, protection, and mitigation provisions and arguments have been validated, and therefore that the AP1000 plant design is robust, being tolerant to faults arising from internal hazards, and that the designed safety measures are effective. |
| I.8. | For each identified hazard combination sequence, the analysis should also consider any deterioration or damage to SSCs important to safety (including hazard barriers) after being subjected to each of the various hazards. For example, for a pipe failure that leads to a missile and a subsequent flood, the analysis of the capability of a hazard barrier to withstand the hydrostatic loads from flooding will need to take account of any damage caused by successive or simultaneous hazards (e.g. the failure of pressurized parts, which could lead to pipe whip, jets, and steam pressure effects on barriers or other SSCs important to safety). | COM | The AP1000 plant design addresses internal and external hazards as described in responses to Sections/Paragraphs 2.1, 2.2 and 3.1. Safety functions will continue to be delivered following various design basis combined hazards through a combination of provisions made on structural barriers, equipment qualification and systems.  Throughout the AP1000 plant, a combination of measures designed to prevent, protect and mitigate the consequences of internal hazards ensures that the safety functions can continue to be delivered and, as such, reduces risk to a level which is ALARP. |
| I.9. | When considering the likelihood of a hazard combination, it should be noted that the initial hazard might put the plant into a state where the second hazard is more likely than its assumed normal frequency. | COM | Independent internal hazards have been assessed as within the design basis where the best estimate initiating event frequency for the two (or more) hazards is greater than 1.0 E-5/reactor year. Combinations of internal hazards with an initiating event frequency less than 1.0 E-5/reactor year are either considered for cliff edge effects or screened from further consideration where the combined initiating event frequency is less than the BSO benchmark. |
| I.10. | Combined hazards can create unique challenges, even if the hazards occur at different areas of the plant or at slightly different times. For example, a fire in a switchgear room could disable flood isolation equipment: this would create a challenge even if the flood were to occur at a later time or in a different room. | NR | This is a statement not a requirement. |
| I.11. | Following screening, some hazard combinations could be selected to be credible but will still need to be assessed against specific acceptance criteria. | COM | See responses to Sections/Paragraphs I.5 and I.6. |

## 

## 2.6. APPENDIX II - DETAILED GUIDANCE ON INTERNAL FIRES

| **Section/Paragraph** | **Requirement**  **Note:** The references noted in [] in column “Requirement” do not relate to the reference list in Sections 4.0 of this document but relate to the reference list of the IAEA Specific Safety Guide SSG-64. | **Compliance** | **Justification** |
| --- | --- | --- | --- |
| **FIRE HAZARD ANALYSIS** | | | |
| II.1. | The fire hazard analysis should be developed on a deterministic basis, with the following assumptions:  (a) A fire is postulated wherever fixed or transient combustible material could be present.  (b) Only one fire is postulated to occur at any one time; consequent fire spread should be considered as part of this single event, if necessary.  (c) The fire is postulated whatever the normal operating status of the plant, whether at power or during shutdown. | COM | A deterministic fire protection analysis is provided in DCD [2] Appendix 9A. The fire protection analysis evaluates the potential for occurrence of fires within the plant and documents the capabilities of the FPS and the capability to safely shut down the plant. |
| II.2. | The fire hazard analysis should take into account any credible combinations of fire and other events, as described in Appendix I. | COM | This is considered in the analysis. |
| II.3. | Simultaneous unrelated fires occurring in different fire compartments, in particular if occurring at a multiple unit site, need not be considered in the design of fire protection means; however, the possibility of a fire spreading from one unit to another unit, or to another installation on the site, should be taken into account in the fire hazard analysis. | OR | The licensing basis for the AP1000 plant is a one-unit application. See Section 2.2 of the DCD [2] for a discussion of accidents external to the nuclear plant (including fires) and the Owner’s responsibility for performing analysis of these events. |
| II.4. | The fire hazard analysis should have the following purposes:  (a) To identify the type and amount, as well as the location and distribution, of fire loads (fixed and transient) and potential ignition sources in the room or plant area.  (b) To identify the relevant items important to safety and to establish the locations of individual components (e.g. control or power cables) in fire compartments.  (c) To analyse the anticipated growth and consequences of a fire with respect to the items important to safety. Assumptions and limitations applicable to the methods of analysis should be clearly stated.  (d) To determine the necessary fire resistance rating of fire barriers. In particular, the fire hazard analysis should be used to determine the necessary fire resistance rating of the boundaries of the fire compartments.  (e) To determine the passive and active fire protection means necessary to achieve safety against fire.  (f) To identify cases in which additional fire separation or fire protection is necessary, in particular for common cause failures, so as to ensure that the necessary functions of items important to safety after a fire are not impaired during and following a credible fire. Moreover, in those plant areas where it is not possible to have fire compartments, the fire hazard analysis should be used for determining the extent of the passive and active protection means necessary to separate the fire cells (the fire influence approach). | COM | a) Each fire area and fire zone is surveyed to determine the type, quantity, and distribution of in-situ combustible materials. Where the presence of transient combustibles is anticipated (for example, materials required to support refueling activities or scheduled maintenance) these materials are also identified.  b) The fire protection analysis identifies safe shutdown components within each of the fire areas.  c) The fire protection analysis includes an assessment of the effects of postulated fires on the ability of the operator to achieve a safe shutdown of the plant.  d) The fire protection analysis considers the need for fire barriers.  e) The fire protection analysis considers the type of fire detection and type of suppression required for each area.  f) The AP1000 plant design includes separate redundant safe shutdown components and associated electrical divisions to preserve the capability to safely shut down the plant following a fire. This is validated by the fire protection analysis. |
| II.5. | The secondary effects of fires and of fire suppression should be evaluated in order to ensure that these effects would not have any adverse effect on safety. | COM | These items are included in the fire protection analysis. |
| II.6. | Detailed guidance on the preparation of a fire hazard analysis is given in Ref. [20]. | NR | This is a statement not a requirement. |
| II.7. | The fire hazard analysis should be complemented by fire probabilistic safety assessment, which has been used in many nuclear power plants to identify and rank the risks of fire. Probabilistic safety assessment could also be used in the design stage to support decision making in the deterministic design of plant layout and fire protection systems. Recommendations on the use of probabilistic safety assessment are provided in IAEA Safety Standards Series No. SSG‑3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants [21]. | COM | A deterministic fire protection analysis is provided in DCD [2] Appendix 9A. In addition, a fire risk assessment was performed as discussed in Chapter 57 [4] of the overall Probabilistic Risk Assessment (PRA) for the AP1000 plant. |
| **FIRE BARRIERS** | | | |
| II.8. | The overall purpose of fire barriers in nuclear power plants is to provide a boundary around a space (e.g. a fire compartment) with a demonstrated capability to withstand and contain an expected fire without allowing the fire to propagate across to, or otherwise cause direct or indirect damage to, materials or items on the side of the fire barrier not exposed to the fire. The fire barrier is expected to perform this function independently of any fire extinguishing action. | COM | Fire barriers are provided in accordance with BTP CMEB 9.5-1 [5]. The AP1000 fire safety design has been achieved by ensuring that a fire is prevented from spreading between redundant trains of equipment utilizing appropriate combinations of physical separation, partial fire-resistant barriers, and fire barriers, including safety-related nuclear fire barriers. |
| II.9. | The fire resistance of fire barriers is characterized by stability, integrity and insulation under fire conditions. The corresponding physical criteria are as follows:  (a) Mechanical resistance;  (b) Capacity to withstand flames, hot gases and flammable gases;  (c) Thermal insulation that is considered satisfactory when the temperature of the unexposed face remains below a prescribed value (e.g. 140°C on average, and 180°C at any one point) over a defined period of time.  The absence of relevant emissions of flammable gases from the face unexposed to the fire should also be verified. | COM | Fire barriers are provided in accordance with BTP CMEB 9.5-1 [5]. Examination, maintenance, inspection, and testing of fire barriers and their penetrations will be actively managed and undertaken in accordance with the relevant plant schedules and local codes. |
| II.10. | Fire barriers can be categorized according to three performance criteria, depending on their specific function and their potential role in a fire, as follows:  (a) Load bearing capability (stability): The ability of a specimen of a load bearing element to support its test load, where appropriate, without exceeding specified criteria for the extent of deformation, the rate of deformation, or both.  (b) Integrity: The ability of a specimen of a separating element to contain a fire with regard to specified criteria for collapse and freedom from holes, cracks and fissures, and sustained flaming on the unexposed face.  (c) Insulation: The ability of a specimen of a separating element to restrict the temperature rise of the unexposed face to below specified levels. | NR | This is a statement not a requirement. |
| II.11. | Within each of the categories in para. II.10, the fire classification of the components is expressed as a ‘rating’ (in minutes or hours) corresponding to the period of time for which the components continue to perform their function when subjected to a thermal test programme in accordance with the standards of the International Organization for Standardization (see Ref. [22]) or other relevant standards. | NR | This is a statement not a requirement. |
| II.12. | The specific functions (load bearing capacity, integrity and insulation) and ratings (e.g. 90 min, 120 min, 180 min) of fire barrier elements (e.g. walls, ceilings, floors, doors, dampers, penetration seals) should be specified in the fire hazard analysis. | COM | The fire protection analysis contains a description of plant fire areas, fire zones, fire barriers, and the protection of fire barrier openings, as well as a description of the separation between redundant safe shutdown components. |
| **FIRE CONTAINMENT APPROACH** | | | |
| II.13. | A fire compartment is a building or part of a building that is completely surrounded by fire resistant barriers: all walls, the floor and the ceiling. The fire resistance rating of the barriers should be sufficiently high that total combustion of the fire load in the compartment can occur (i.e. total burnout) without breaching the fire barriers. | COM | The fire barriers are constructed to withstand the complete combustion of the fire load within the enclosure (full-room burnout), thereby preventing the fire from propagating across to, or otherwise causing direct or indirect damage to, materials or items on the sides of the fire barrier that are not exposed to the fire. This prevents the effects of a fire in one compartment from damaging redundant SSCs located in adjacent fire compartments. |
| II.14. | Redundant items important to safety should be located in separate fire compartments, in order to implement the concept of segregation, as described in Section 4, and to separate them from high fire loads and other fire hazards. This preferred method is referred to as the ‘fire containment approach’. Confinement of the fire within the fire compartment should prevent the spread of fire and its (direct and indirect) effects from one fire compartment to another, and thus prevent the failure of redundant items important to safety. The separation provided by fire barriers should not be compromised by the effects of fire or fire by‑products, or by pressure effects of fires on common building elements such as building services or ventilation systems. | COM | To prevent the spread of fires, passive fire protection measures such as fire-resistant barriers and physical or spatial separation are used in the fire protection design of AP1000 plant. Fire compartmentalization is used extensively throughout AP1000 plant. The quantity and arrangement of the combustible materials in the fire zones, and the characteristics of the barriers that separate one zone from other zones are such that a fire which damages safe shutdown components in one zone does not propagate to the extent that it damages redundant safe shutdown components in another fire zone. |
| II.15. | Since any penetration of a barrier can reduce its overall effectiveness and reliability, such penetrations should be minimized, in particular between different redundant divisions. The fire resistance rating of any devices for closing passages, such as doors, ductwork, hatches, and pipe and cable entryway seals, that form part of a fire barrier and a fire compartment boundary should be at least equal to the fire resistance necessary for the fire barrier itself. | COM | Openings through fire barriers for pipe, conduit, and cable trays that separate fire areas are sealed or closed to provide a fire resistance rating equal to that required of the barrier.  Door openings in fire barriers are protected with equivalently rated doors, frames, and hardware. Fire doors are self-closing or provided with closing mechanisms.  Penetration openings for ventilation systems are protected in accordance with NFPA 90A [13]. Fire barrier penetration openings for ventilation are protected by fire dampers having a rating equivalent to that of the fire barrier. Fire dampers are generally not provided for roof or exterior wall penetrations. |
| II.16. | If the fire containment approach is followed, the provision of fire extinguishing systems to meet Requirement 17 and the requirements established in para. 5.16 of SSR‑2/1 (Rev. 1) [1] is not necessary (see also paras 4.30–4.34). Nevertheless, such provisions should be installed where there is a high fire load, as determined by the fire hazard analysis, in order to confine a fire as soon as possible. | COM | Compliance of the AP1000 plant with IAEA SSR-2/1 is documented in [7].  The primary objectives of the AP1000 plant fire protection program are to prevent fires and to minimize the consequences should a fire occur. |
| II.17. | Other design requirements might prevent the full adoption of the fire containment approach throughout the design of a nuclear power plant. This might be the case, for example, in the following areas:  (a) In areas such as the reactor containment and in control rooms of certain designs, where redundant divisions of safety systems could be located close to each other in the same fire compartment;  (b) In areas where the use of structures to form fire barriers could unduly interfere with normal plant functions such as plant maintenance, access to equipment and in‑service inspection.  In areas where individual fire compartments cannot be utilized to separate items important to safety, protection can be provided by locating the items in separate fire cells. This is known as the ‘fire influence approach’. Figure 1 illustrates applications of the fire containment approach and the fire influence approach. | NR | This is a statement not a requirement. |
| **FIRE INFLUENCE APPROACH** | | | |
| II.18. | Fire cells are separate areas in which redundant items important to safety are located. Since fire cells might not be completely surrounded by fire barriers, spreading of fire between cells should be prevented by other means of protection. These means include the following:  (a) The limitation of combustible materials;  (b) The separation of equipment by distance, without intervening combustible materials;  (c) The provision of local passive qualified fire protection such as fire shields or cable wraps;  (d) The provision of fire detection and extinguishing systems. | COM | a) The AP1000 plant is designed to prevent fire initiation by controlling, separating, and limiting the quantities of combustibles and sources of ignition.  b) Redundant safe shutdown components and associated electrical divisions are separated to preserve the capability to safely shut down the plant following a fire.  c) See Section/Paragraph II.14.  d) See responses to Sections/Paragraphs:   * “Fire detection and alarm systems” II.33 – II.40. * “Fire extinguishing means” from II.41 – II.74. |
| II.19. | Combinations of active and passive means could be used to achieve a satisfactory level of protection; for example, the use of fire barriers (walls, ceilings, floors, doors, dampers, penetration seals and cable wraps) and their fire rating should be specified in the fire hazard analysis together with an extinguishing system. | COM | The AP1000 plant design provides combination of active and passive means to achieve a satisfactory level of protection. |
| II.20. | The fire hazard analysis should demonstrate that protection measures are sufficient to prevent the failure of redundant items important to safety that are located in separate fire cells. | COM | This is demonstrated in the fire hazard analysis. See also response to Section/Paragraph II.14. |
| II.21. | Where separation by distance is the sole means of protection between fire cells, the fire hazard analysis should demonstrate that neither radiative nor convective heat transfer effects nor fire by‑products would jeopardize the separation. | COM | Detailed analysis of the fire segregation and separation approaches adopted in the AP1000 plant design has been undertaken. See DCD [2] Appendix 9A. |
| **ACCESS ROUTES AND ESCAPE ROUTES** | | | |
| II.22. | Adequate access and escape routes for personnel need to be provided, with account taken of the requirements of national building codes, fire protection regulations and rules for accident prevention, as well as the recommendations of this Safety Guide. Ideally, a minimum of two escape routes from every building should be provided. For each route the following general conditions should be met:  (a) Access routes and escape routes should be protected from the effects of fire and fire by‑products. Protected access routes and escape routes comprise staircases and passageways leading to an exit from the building.  (b) Access routes and escape routes should be kept clear of any stored material.  (c) Fire extinguishers should be placed at appropriate locations along the access routes and escape routes, as required by national regulations.  (d) Access and escape routes should be clearly and permanently marked and should be easy to recognize. The markings of access routes and escape routes should show the shortest possible safe routes.  (e) The floor level or number should be clearly marked on all staircases.  (f) Emergency lighting should be provided on access routes and escape routes.  (g) Appropriate means for raising the alarm (e.g. fire call points) should be available at all places that have been defined in a hazard analysis (i.e. fire hazard analysis), and on all escape routes and building exits.  (h) Access and escape routes should have the capability to be ventilated, by either mechanical or other means, to prevent smoke accumulating and to facilitate access.  (i) Staircases that serve as access routes and escape routes should be kept free of all combustible materials. Overpressure ventilation could be necessary in order to keep the staircase free of smoke. It is advisable to make provision for smoke removal from corridors and rooms leading to staircases. For high, multi‑storey staircases, consideration should be given to subdividing the staircase.  (j) Doors leading onto staircases or access routes and escape routes should be of the self‑closing and self‑latching type and should open in the direction of escape.  (k) Means should be provided to allow quick evacuation of the reactor containment through airlocks. The measures should be adequate to deal with the largest number of personnel expected to be present during maintenance periods and outages.  (l) A reliable communication system should be provided for all access routes and escape routes.  (m) All emergency lighting systems should be energized at all times and should be provided with non‑interruptible emergency power supplies. | COM  OR  POS | Firefighting personnel access routes and life safety escape routes are provided for each fire area; therefore, the design accommodates these routes.  The AP1000 plant design accounts for clearly marked escape routes, equipped with lighting and ventilation, exit doors and stairwells. The basic design criteria for egress and life safety for the AP1000 plant is identified in APP-GW-A1-103 [26]. Egress studies have been conducted for the standard AP1000 plant in APP-GW-A2R-001 [27] and APP-G1-A2R-001 [28]. Project-specific egress studies will need to be performed to reflect the final design of the AP1000 units for a specific site. The Owner shall be responsible for development of site-specific evacuation routes. |
| **PROTECTION AGAINST ELECTRICAL CABLE FIRES** | | | |
| II.23. | The large inventories of organic insulated electrical cable constitute a significant source of combustible material in nuclear power plants. The impact of electrical cable fires on items important to safety should be determined in the fire hazard analysis. | COM | This is considered in the fire protection analysis. |
| II.24. | Various design approaches have been taken to limit the significant impact of cable fires. Among these approaches are the following:  (a) Protecting electrical circuits against overload and short circuit conditions;  (b) Limiting the total inventory of combustible material in cable installations;  (c) Reducing the relative combustibility of cable insulation;  (d) Providing fire protection to limit fire propagation;  (e) Providing separation between cables from redundant divisions of safety systems, and between power supply cables and control cables. | NR | This is a statement not a requirement. |
| II.25. | Design approaches should be taken to limit the significant impact of cable fires as follows:  (a) Providing fire protection to limit fire propagation.  (b) Providing segregation between cables from redundant divisions of safety systems.  (c) Providing segregation between power supply cables and control cables, as far as practicable. Where segregation is not possible, separation may be appropriate. | COM | a) Water based fire protection system is provided as the primary fire suppression for cable fires.  b) Redundant safety-related cable systems are separated from each other and from potential fire exposure hazards in non-safety-related areas by 3-hour rated fire barriers.  c) There are five separation groups for the cable and raceway system: groups A, B, C, D, and N. Separation group A contains safety-related circuits from division A. Similarly, separation group B contains safety-related circuits from division B; group C from division C; group D from division D; and group N from non-safety-related circuits. Cables of one separation group are run in separate raceways and physically separated from cables of other separation groups. Group N raceways are separated from safety-related groups A, B, C, and D. Raceways from group N are routed in the same areas as the safety-related groups according to spatial separation stipulated in Regulatory Guide 1.75, ”Physical Independence of Electric Systems” [29] and IEEE 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits” [16].  Separate raceways are provided for medium voltage power, low voltage power, and control, as well as instrumentation cables. |
| II.26. | Care should be taken to ensure that cables serving items important to safety are not routed over designated storage areas or other areas of high fire hazard. | COM | Raceways are kept at a reasonable distance from heat sources such as steam piping, steam generators, boilers, high and low pressure heaters, and any other actual or potential heat source. Cases of heat source crossings are evaluated and supplemental heat shielding is used if necessary.  The design ensures that piping for flammable or combustible liquids or gases does not create any potential exposure hazard to important cable systems. |
| **CONTROL OF CABLE FIRES** | | | |
| II.27. | Controls should be imposed on the quantities of combustible cable insulation (e.g. polymer insulation) installed on cable trays and within cable routes. These controls are necessary to prevent the fire load exceeding the rated resistance of compartment fire barriers and to minimize the rate of spread of fire along cable trays. The controls should include limits on the numbers and sizes of cable trays and/or the loading of insulation upon them, and should correspond to the combustion characteristics of the cables used. | COM | The insulating and jacketing material for electrical cables is selected to meet the fire and flame test requirements of IEEE 383 [16], “IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations,” or IEEE 1202 [15], “IEEE Standard for Flame Testing of Cables for Use in Cable Tray in Industrial and Commercial Occupancies”, excluding the option to use flame source, oil, or burlap. |
| **CABLE FIRE TESTING** | | | |
| II.28. | The qualification tests for fire retardant electrical cables vary across different national standards; however, large scale flame propagation tests for cables often involve exposing vertical or horizontal cable samples to a flaming ignition source. Among the important variable factors associated with cable fire tests are the following:  (a) The cable inventory as an ignition source;  (b) Cable layout, in particular configurations with multiple cable trays;  (c) Resistance to ignition;  (d) Extent of fire propagation;  (e) Air flow rate;  (f) Thermal isolation of the enclosure;  (g) Toxicity and corrosiveness associated with smoke formation. | COM  POS | Electric cable construction will pass the flame test in IEEE 1202 [15] or IEEE 383 [16], excluding the option to use the alternate flame source, oil, or burlap. |
| **CABLE FIRE PROTECTION** | | | |
| II.29. | In some circumstances, specific passive protection measures should be provided to protect electrical cables from fire. Such measures include the following:  (a) Cable coatings to reduce the potential for ignition and to delay flame propagation;  (b) Cable wraps to provide segregation from other fire loads and from other systems and/or items important to safety;  (c) Fire stops to limit flame propagation.  Since these measures can lead to overheating of the cable and derating of the current load, these factors should be taken into account in determining the choice of materials to be used. | COM | Passive protection measures will be provided where necessary. See DCD [2] Section 9.5 and Appendix 9A. |
| II.30. | The potential impact of cable fires can be reduced by providing suitable segregation using the fire containment approach (see paras II.13–II.17). | NR | This is a statement not a requirement. |
| II.31. | In some cases, physical separation with no intervening combustible materials (alone or in conjunction with fire safety measures) can provide sufficient protection to preclude damage to redundant items important to safety due to a single credible fire. It is not possible to specify a single minimum distance that would provide adequate safe separation for all circumstances, but rather the adequacy of the separation should be determined by carefully analysing the particular situation. | COM | Separate raceways are provided for medium voltage power, low voltage power, and control, as well as instrumentation cables. The design, routing, and separation of cable and raceways are further described in DCD [2] Section 8.3. |
| II.32. | The preferred approach for the separation of redundant divisions of a safety system should be the fire containment approach. | COM | See response to Section/Paragraph II.25. |
| **FIRE DETECTION AND ALARM SYSTEMS** | | | |
| II.33. | The nature of the fire detection and alarm systems, their layout, the necessary response time and the characteristics of their detectors, including their diversification, should be determined by the fire hazard analysis or system design requirements. | COM | 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 [13]. Fire detection and alarm systems are generally in accordance with NFPA 804 [13]. See WCAP-15871 [14] for details.  The types of fire detectors used in specific applications are identified in the fire protection analysis. |
| II.34. | The fire detection and alarm systems should provide information in the control room about the location and spread of a fire by means of audible and visual alarms. Local audible and visual alarms, as appropriate, should also be provided in plant areas that are normally occupied. Fire alarms should be distinctive to prevent them being confused with any other alarms in the plant. | COM | The fire detection system provides audible and visual alarms and system trouble annunciation in the main control room and the security central alarm station. |
| II.35. | Detection and alarm systems should be functional at all times and should be provided with non‑interruptible emergency power supplies, including fire resistant supply cables where necessary. Recommendations on emergency power supplies are provided in SSG‑34 [7] | COM | Each fire detection, indicating, and alarm unit is provided with reliable ac electrical power from the non-Class 1E uninterruptible power supply system. These are backed up by the diesel generators and battery systems. |
| II.36. | Individual detectors should be sited so that the flow of air due to ventilation or pressure differences provided for contamination control will not cause smoke or heat energy to flow away from the detectors and thus unduly delay actuation of the detector alarm. Fire detectors should also be placed in such a way as to avoid spurious signals due to air currents generated by the operation of the ventilation system. This should be verified by in situ testing where feasible. | COM | The AP1000 plant design meets the requirement. |
| II.37. | In the selection and installation of fire detection equipment, account should be taken of the environment in which the equipment will function (e.g. in terms of radiation fields, humidity, temperature and air flow). If the environment does not allow detectors to be placed in the immediate area to be protected (e.g. owing to increased radiation levels or high temperatures), alternative methods should be considered, such as the sampling of the atmosphere from the protected area for analysis by remote detectors with automatic operation. | COM | Fire detectors are selected and installed in accordance with NFPA 72 [13]. The selection and installation of fire detectors is also based on consideration of the type of hazard, combustible loading, the type of combustion products, and detector response characteristics. The types of detectors used in each fire area are identified in the fire protection analysis. |
| II.38. | Wiring for fire detection systems, alarm systems or actuation systems should include the following features:  (a) Protection from the effects of fire by a suitable choice of cable type, by proper routing, by a looped configuration or by other means;  (b) Protection from mechanical damage;  (c) Constant monitoring for integrity and functionality. | COM | Fire detection and alarm systems are provided where required by the fire protection analysis, in accordance with BTP CMEB 9.5-1 [5] and NFPA 72, “National Fire Alarm Code” [13]. Fire detection and alarm systems are generally in accordance with NFPA 804 [13]. |
| **SELECTION AND LOCATION OF DETECTORS** | | | |
| II.39. | The types of fire detector to be installed should be carefully selected, as should their location and positioning, to ensure that the detectors will actuate as expected in response to a fire. Numerous factors affect the response of fire detectors to the growth of a fire, including the following:  (a) Burning rate;  (b) Rate of change of the burning rate;  (c) Characteristics of the burning materials;  (d) Ceiling height;  (e) Positions and locations of detectors;  (f) Locations of walls;  (g) Positions of any obstructions to gas flow;  (h) Room ventilation;  (i) Response characteristics of the detector | COM | Fire detectors respond to smoke, flame, heat, or the products of combustion. The installation of fire detectors is in accordance with NFPA 72 [13] and the manufacturer's recommendations. The selection and installation of fire detectors is also based on consideration of the type of hazard, combustible loading, the type of combustion products, and detector response characteristics. The types of detectors used in each fire area are identified in the fire protection analysis. |
| II.40. | Analyses should be performed to evaluate the effectiveness of the selected type and locations of the fire detectors. | COM | The types of detectors used in each fire area are identified in the fire protection analysis. See also response to Section/Paragraph II.33. |
| **FIRE EXTINGUISHING MEANS** | | | |
| **FIXED PROVISIONS FOR FIRE EXTINGUISHING** | | | |
| II.41. | Nuclear power plants should be provided with fixed fire extinguishing equipment. This should include provisions for manual firefighting, such as fire hydrants and fire standpipes. | COM | The fire protection system consists of a number of fire detection and suppression subsystems, referred to as systems, including:   * Detection systems for early detection and notification of a fire * A water supply system including the fire pumps, yard main, and interior distribution piping * Fixed automatic fire suppression systems * Manual fire suppression systems and equipment, including hydrants, standpipes, hose stations and portable fire extinguishers |
| II.42. | The fire hazard analysis should determine the need to provide automatic extinguishing systems such as sprinklers; spray systems; foam, water mist or gaseous systems; or dry chemical systems. The design criteria for fire extinguishing systems should be based on the findings of the fire hazard analysis, so as to ensure that the design is appropriate for each fire hazard that is being protected against. | COM | Fixed automatic fire suppression systems are provided based on the results of the fire protection analysis. Automatic fire suppression systems are in accordance with BTP CMEB 9.5-1 [5] and the applicable NFPA standards. This is with consideration of the unique aspects of each application, including building characteristics, materials of construction, environmental conditions, fire area contents, and adjacent structures. |
| II.43. | Fire extinguishing systems should be designed and located to ensure that neither their intentional operation nor their spurious operation would jeopardize the function of SSCs important to safety (including safety features for design extension conditions). | COM | For fire areas containing safety-related components, the potential for a credible inadvertent actuation of automatic suppression systems is determined and the consequences are evaluated. The result is that inadvertent actuation of the FPS does not prevent plant safety functions from being performed. |
| II.44. | Consideration should be given in the design to the potential for errors in the operation of extinguishing systems. Consideration should also be given to the effects of discharges from extinguishing systems in locations adjacent to the fire compartment where the fire started. | COM | To achieve the required high degree of fire safety, and to satisfy fire protection objectives, the AP1000 plant is designed to provide confidence that failure or inadvertent operation of the fire protection system cannot prevent plant safety functions from being performed. As part of the fire protection analysis, for fire areas containing safety-related components, the potential for a credible inadvertent actuation of automatic suppression systems is determined and the consequences are evaluated. |
| II.45. | In the selection of the type of extinguishing system to be installed, consideration should be given to the necessary response time, the characteristics regarding its capability for extinguishing a fire (e.g. thermal shock) and the consequences of operation of the system for plant personnel and for items important to safety, as established by the fire hazard analysis. | COM | Extinguishing systems are selected in accordance with the fire protection analysis. |
| II.46. | In general, water systems should be preferred in areas containing high fire loads, where there is a possibility of firmly established fires, and where cooling is necessary. Automatic sprinklers, water mist systems, water spray and deluge systems as well as water based foam systems should be used in cable spreading rooms and storage areas, and to protect equipment containing large quantities of oil, such as turbogenerators and oil cooled transformers. Water mist and foam systems are more complex. Water mist has the advantage of discharging smaller quantities of water to achieve control. Gaseous extinguishing systems are usually used in locations containing control cabinets and other electrical equipment susceptible to water damage. | COM | The selection of suppression equipment considers many factors including the amount of combustible material present and the spread of contamination. The method of suppression for each area is described in the fire protection analysis. |
| II.47. | For prompt operation and availability at the time of a fire, automatic extinguishing systems are preferred. However, provision should be made for the manual actuation of automatic systems. Provision should also be made for manual shut‑off of automatic systems, to permit the termination of spurious discharges or the control of water runoff or other side effects. | COM | Operation of the automatic systems is discussed and justified in the fire protection analysis. See Appendix 9A in the DCD [2]. |
| II.48. | The exclusive use of manually operated extinguishing systems should only be acceptable if the evaluation in the fire hazard analysis demonstrates that the anticipated delay in manual actuation would not result in unacceptable damage. | COM | This is considered in the fire protection analysis. |
| II.49. | Any fixed extinguishing system that is solely manually actuated should be designed to withstand fires for a sufficient period of time to allow for the manual actuation. | CWO | The fire protection system is classified as a non-safety-related, non-seismic system. Special seismic design requirements are applied to portions of the standpipe system located in areas containing equipment required for safe shutdown following a safe shutdown earthquake, as described in DCD [2] Section 9.5.1.2.1.5. The fire protection system is not required to remain functional following a plant accident or the most severe natural phenomena, except for a safe shutdown earthquake. |
| II.50. | All parts, except for the detection devices themselves, of any electrical activation system or electrical supplies for fire extinguishing systems should be protected from fire or should be located outside the fire compartments protected by the systems. Failure of the electrical supply should give rise to an alarm. | N/A | Electrical activation system or electrical supplies for fire extinguishing systems are not used in the AP1000 plant design. |
| II.51. | For all fire extinguishing systems, an operational test is usually necessary in commissioning, either by means of actual discharge tests or by the use of equivalent methods. | OR | Recommendations for preoperational, startup, and surveillance procedures will be provided by Westinghouse. However, the testing program for fire protection shall be the responsibility of the Owner. |
| II.52. | A formal maintenance, testing and inspection programme should be established in order to provide assurance that fire protection systems and components function correctly and meet the design requirements. Further recommendations on the implementation of this programme are provided in IAEA Safety Standards Series No. NS‑G‑2.1, Fire Safety in the Operation of Nuclear Power Plants [23]. | OR | The Owner shall be responsible for testing and inspection during plant operation. |
| **WATER BASED EXTINGUISHING SYSTEMS** | | | |
| II.53. | Water based extinguishing systems should be permanently connected to a reliable and adequate supply of fire extinguishing water. | COM | The fire protection system normally operates in an active standby mode. The fire water supply piping is kept full and pressurized by operation of the jockey pump. When water pressure in the yard main begins to fall, due to a demand for water from automatic or manual suppression systems, the motor-driven pump starts automatically on a low-pressure signal. If the motor-driven pump fails to start, the diesel-driven pump starts upon a lower pressure signal. The pump continues to run until it is stopped manually. See also responses to Section/Paragraphs II.70 and II.71. |
| II.54. | Water based automatic fire extinguishing systems include sprinkler, water spray, deluge, foam and water mist systems. Subject to the findings of a fire hazard analysis, automatic protection should be provided at all locations where one of the following factors applies:  (a) A high fire load is present;  (b) A potential for rapid spread of fire exists;  (c) A fire could compromise redundant items important to safety;  (d) An unacceptable hazard for firefighters could be created;  (e) An uncontrolled fire would make access for firefighting difficult. | COM | The selection of suppression equipment considers many factors including the amount of combustible material present and the spread of contamination. The method of suppression for each area is described in the fire protection analysis. |
| II.55. | If the fire hazard analysis indicates that water alone might not be suitable for successfully coping with the hazard (e.g. in the case of application to flammable liquids), consideration should be given to systems using fire extinguishing foam. | N/A | Foam suppression systems are not used on AP1000 plant design. |
| II.56. | In addition to the expected fire exposure as determined in the fire hazard analysis, various factors should be addressed in the design of water sprinkler systems, such as adequate type and location of sprinkler heads or spray nozzles. | COM | Automatic sprinkler and water spray systems are provided in accordance with the applicable requirements of NFPA 13 and NFPA 15 [13]. |
| II.57. | The component parts of water based systems should be constructed from compatible materials in order to avoid galvanic corrosion. | COM | The materials used in the water-based systems are resistant to galvanic corrosion, and they are consistent with applicable industry guides, standards, and criteria. |
| II.58. | Where water based extinguishing systems are used, means should be provided to confine potentially contaminated water, and adequate drains should be provided with arrangements to prevent any uncontrolled release of radioactive material to the environment. | COM  OR | Floor drains are provided, which are sized to remove expected firefighting water flow without flooding safety-related equipment. Fire-fighting water will be collected in the sumps for each of the buildings. Water within containment and the radiologically controlled area of the auxiliary building will ultimately be discharged through the liquid radwaste system (WLS). Water within the other buildings will be discharged through the waste water system. The sumps allow for sampling and the discharges are monitored. The Owner shall be responsible for ensuring that water drainage from areas that may contain radioactivity are collected, sampled, and analyzed before discharge to the environment. The Owner shall be responsible for disposal of any other fire-fighting media. |
| **FIRE HYDRANT, STANDPIPE AND HOSE SYSTEMS** | | | |
| II.59. | Reactor buildings should be provided with a fire standpipe and hose system (dry risers). | COM | Wet standpipe systems are used except inside containment. The portion of the system inside containment is a dry standpipe system. For more information, see DCD [2] Section 9.5.1.2.1.5. |
| II.60. | The fire hydrant system for the reactor building should have provisions for local or remote actuation. | CWO | The fire hydrant system for containment building can be activated manually. Remote actuation is not required because continuous water supply is provided in the fire protection system. |
| II.61. | The distribution loop for fire hydrants should adequately provide for exterior firefighting operations on all buildings. Internal standpipes with a sufficient number of fire hoses of sufficient length, and with connections and accessories adequate for the hazard, should be provided to cover all interior areas of the plant, unless duly justified by the fire hazard analysis. | COM | Hydrants are provided on the yard main in accordance with NFPA 24, “Standard for Installation of Private Fire Service Mains and Their Appurtenances” [13] at intervals of up to about 250 feet (76.2 m). They provide hose stream protection for every part of each building and two hose streams for every part of the interior of each building not covered by standpipe protection, excluding certain remote areas of the shield building. |
| II.62. | Each hydrant hose and standpipe riser should have connections that are compatible with on‑site and off‑site firefighting equipment. | COM  POS | All hose threads will be compatible with the local standards. |
| II.63. | Suitable accessories such as fire hoses, adapters, foam mixing devices and nozzles should be provided at strategically located points throughout the plant, as identified in the fire hazard analysis. The accessories should be compatible with those of external fire services. | COM  POS | All accessories will be compatible with the local standards. |
| II.64. | The fire extinguishing water supply system to each separate building should be provided with no fewer than two independent hydrant points. Each building supply should be provided with an indicating shut‑off valve. | COM | Design considerations for plant’s hydrant points are discussed in DCD [2] Section 9.5. See also response to Section/Paragraph II.61. |
| **WATER SUPPLY SYSTEM FOR FIRE EXTINGUISHING EQUIPMENT** | | | |
| II.65. | The main loop of the water supply system for the fire extinguishing equipment should be designed to supply the anticipated demand for water: see para. II.70. The distribution of water to the fire extinguishing equipment should be through a main loop such that water can reach each connection from two directions. | CWO | Fire protection water is distributed by an underground yard main loop, designed in accordance with NFPA 24, “Standard for Installation of Private Fire Service Mains and Their Appurtenances” [13]. Sprinkler and standpipe systems are supplied by connections from the yard main. Where plant areas (other than the containment and outlying buildings) are protected by both sprinkler systems and standpipe systems, the connections from the yard main are arranged so that a single active failure or a crack in a moderate energy line cannot impair both systems.  See also response to Section/Paragraph II.70. |
| II.66. | Valves should be provided to isolate the water in parts of the main loop. Local visual indications of whether the valves are open or closed should be provided. Valves in the main loop should be so arranged that closure of a single valve does not cause the complete loss of capability of the fire extinguishing system in any given fire compartment, unless this is indicated by the recommendations of the fire hazard analysis. The loop valves for the fire extinguishing water should be located sufficiently far from the hazard against which they are protecting so as to remain unaffected by a fire in that area. | COM | Indicator valves are provided for sectionalized control and isolation of portions of the yard fire main loop. Valves are installed to permit isolation of outside hydrants from the fire main for maintenance or repair without interrupting the water supply to automatic or manual fire suppression systems. |
| II.67. | The water system for the fire extinguishing system should be used only for fire extinguishing. This water system should not be connected into the piping of the service water or sanitary water systems except as a source of backup supplies of firefighting water or to perform a safety function to mitigate an accident condition. Such connections should be provided with an isolating valve that is locked in the closed position or should be provided with position monitoring during normal operation. | COM | The fire protection system does not rely on the operation of another water system as a second water source. |
| II.68. | The fire extinguishing water main loop could serve more than one reactor at a multi‑unit site, and common water supplies could be utilized for such installations. | N/A | See discussion of GDC 5 in DCD [2] Section 3.1.1. The AP1000 is a single-unit plant. |
| II.69. | At sites where pumping is needed to provide the necessary amount of water, fire pumps should be redundant, diverse and separated (i.e. with regard to fire protection) to ensure adequate functionality in the event of equipment failure. Fire pumps should have independent controls, automatic start and manual shut‑off, diverse power supplies provided by the plant’s emergency power supply and independent prime movers (see SSG‑34 [7]). An indication that the pumps are running, together with alarms indicating power failure or failure of the fire pumps, should be provided in the control room. In areas subject to freezing, a low temperature alarm should also be provided. | COM | Two 100 percent capacity fire pumps (one diesel-driven and one electric motor-driven) are provided. Alarms indicating pump running, driver availability, failure to start, and low fire main pressure are provided in the main control room. |
| II.70. | The water supply system for the fire extinguishing system should be designed on the basis of the highest expected flow rate at the necessary pressure for the minimum period of time needed to bring the fire under control. This flow rate, derived from the fire hazard analysis, should be based on the largest water demand for any fixed fire extinguishing system plus an adequate allowance for manual firefighting. In the design of the water supply system for the fire extinguishing system, the minimum pressure at the highest outlet in the plant should be taken into account. Any need to prevent freezing at low temperatures should be taken into account. Consideration should be given to the provision of trace heating or other measures to prevent the freezing of vulnerable pipework. | COM | The FPS is designed to maintain 100 percent of fire pump design capacity, assuming failure of the largest fire pump or the loss of offsite power.  The FPS is designed from one tank to supply fire suppression water at a flow rate and pressure sufficient to satisfy the demand of any automatic sprinkler system plus 500 gpm (114 m3/hr) for fire hoses, for a minimum of 2 hours, in accordance with NFPA 804 [13].  Residual pressure at the hose connection is a minimum of 100 psig (7.0 kg/cm2) in accordance with NFPA 14 [13]. |
| II.71. | Two separate reliable water sources should be provided. If only one water source is provided, then it should be sufficiently large (e.g. a lake, pond or river) and at least two independent intakes should be provided. If only water tanks are provided, two tanks, each capable of meeting the entire demand for water for the system, should be installed. The main plant water supply capacity should be sufficient to allow refilling of either tank within a sufficiently short period of time. Tanks should be capable of being interconnected so that pumps can take water from either tank or both tanks. Each tank should be capable of being isolated in the event of a leak. Tanks should be fitted with fire pump connections. | CWO | Fire water is supplied from two separate fresh water storage tanks. The primary fire water tank is dedicated to the fire protection system. The secondary fire water tank contains water for use by the fire protection system and the containment spray system. The fire water tanks are permanently connected to the fire pumps suction piping and are arranged so that the pumps can take suction from either or both tanks. Piping between the fire water sources and the fire pumps is in accordance with NFPA 20 [13]. A failure in one tank or its piping cannot cause both tanks to drain.  These tanks are redundant, and each can provide fire suppression water at a flow rate and pressure sufficient to satisfy the demand of any automatic sprinkler system plus 500 gpm (114 m3/hr) for fire hoses, for a minimum of 2 hours, in accordance with NFPA 804 [13].  The tanks can be refilled within 8 hours, interconnected, and isolated.  The plant design does not have a dedicated connection for fire engines. However, there is a 150 DN (6-inch) drain line with a raised face flanged end that could potentially be used. |
| II.72. | When a common water supply is provided for fire protection and the ultimate heat sink, the following conditions should also be satisfied:  (a) The necessary capacity for the water supply for the fire protection system should be a dedicated part of the total water inventory.  (b) Failure or operation of the fire protection system should not affect the water supply for the ultimate heat sink (or vice versa), including for combinations of events. | N/A | Common water supply for fire protection and the ultimate heat sink is not used in the AP1000 plant design. |
| II.73. | Where appropriate, measures to prevent the blockage of the sprinklers or their nozzles by debris, biological fouling or corrosion products should be implemented (e.g. chemical treatment, additional filtration). | COM | The source of fire water is the raw water system, which provides chemical treatment and filtration to remove sediment and debris before water is delivered to the fire water storage tanks. |
| II.74. | Provision should be made for the inspection of water supply equipment such as filters, end connections, sprinkler heads and spray nozzles. Water flows should be regularly tested by discharge to provide confidence in the continued ability of the system to perform its intended functions throughout the lifetime of the plant. Precautions should be taken to prevent water damage to electrical equipment during testing. | OR | The Owner shall be responsible for testing and inspection during plant operation. |
| **GASEOUS EXTINGUISHING SYSTEMS** | | | |
| II.75. | Gaseous fire extinguishing systems consist of a gaseous fire suppression agent, a source of compressed gas propellant, an associated distribution network, discharge nozzles and provisions for detection and/or actuation. The systems can be either manually operated at the location of the hazard, or remotely or automatically actuated by a detection system. | NR | This is a statement not a requirement. |
| II.76. | Gaseous extinguishing agents are usually termed clean agents as they leave no residue after deployment. Since they are also non‑conductive, their characteristics make them suitable for protecting electrical equipment. Several types of gaseous extinguishing system are available, and more are under development. The advantages of clean agent systems are offset by the need for the concentration of the agent to be maintained, the complexity of the systems, their inability to provide cooling and the single use nature of their operation. | NR | This is a statement not a requirement. |
| II.77. | Carbon dioxide systems, or any other gaseous systems with the potential for causing a hazard to personnel, should never be used to protect areas that are normally occupied. | N/A | No fixed gas suppression systems are used in the AP1000 plant design due to life safety considerations. |
| II.78. | There are generally two methods of providing protection with gaseous extinguishing agents: local application, where the agent is discharged towards the hazard or a particular piece of equipment; and total flooding, where the agent is discharged into a fire compartment or into enclosed equipment such as switchgear. Some extinguishing agents are unsuitable for local application. | NR | This is a statement not a requirement. |
| II.79. | Considerations for gaseous fire extinguishing systems are as follows:  (a) In determining the need for gaseous extinguishing systems, consideration should be given to the type of fire, possible chemical reactions with other materials, the effects on charcoal filters, and the toxic and corrosive characteristics of the products of thermal decomposition and of the agents themselves.  (b) Gaseous fire extinguishing systems should not be used where cooling is needed, for example to extinguish firmly established fires, such as those in areas containing a high fire load of electrical cable material. When gaseous agents are used, consideration should be given to the possibility of re‑ignition if the concentration of extinguishing medium falls below the minimum necessary level before any residual combustible material has cooled sufficiently.  (c) The total quantity of any gaseous extinguishing agent should be sufficient to extinguish the fire. This is usually accomplished (except for halogenated agents) by means of oxygen dilution. In determining the quantity of agent necessary, account should be taken of the leaktightness of the enclosure, the necessary extinguishing concentration for the hazard, the rate of application and the period for which the design concentration is to be maintained.  (d) To avoid overpressures that would result in structural damage or damage to equipment, the structural effects of the buildup of pressure within protected enclosures resulting from the discharge of gaseous extinguishing agents should be evaluated, and provision should be made for safe venting where necessary. Caution is necessary in selecting venting arrangements so as not to transfer the overpressure or environmental conditions into the relieving area.  (e) Consideration should be given to the potential for damage due to thermal shock when gaseous extinguishing systems are discharged directly onto equipment important to safety. This could occur during local manual applications and during automatic discharges into electrical cabinets. The design should ensure that nozzles are located to avoid fanning the flames of the fire on the initial discharge of the system. | N/A | No fixed gas suppression systems are used in the AP1000 plant design due to life safety considerations. |
| II.80. | Suitable precautions should be taken to protect persons who enter a location where the atmosphere might have become hazardous owing to the inadvertent leakage or discharge of carbon dioxide or any other hazardous gas from an extinguishing system. Such precautions include the following:  (a) Precautions to prevent leakage of carbon dioxide or any other hazardous extinguishing gas in dangerous concentrations to adjacent areas that might be occupied by personnel;  (b) Provision of devices to prevent automatic discharge of the system while personnel are, or could be, within the protected space;  (c) Provision for manual operation of the system from outside the protected space;  (d) Provision of a continuous alarm following the discharge of a gas within the entrances to protected enclosures until the atmosphere has been returned to normal;  (e) Continued operation of the fire detection and alarm system until the atmosphere has been returned to normal (this can help to avoid premature re‑entry with the fire still ignited and can protect personnel from toxic gases);  (f) Means to ventilate protected enclosures after the discharge of the gaseous extinguishing system. Forced ventilation is often necessary to ensure that an atmosphere hazardous to personnel is dissipated and not moved to other areas. | N/A | No fixed gas suppression systems are used in the AP1000 plant design due to life safety considerations. |
| II.81. | Total flooding applications rely on a rapid and even distribution of gas throughout the space that is flooded. This is usually achieved within 10–30 seconds of actuation by the use of special nozzles and a system designed to proprietary specifications. Rapid distribution of gas is particularly important when the gaseous agent is heavier than air, in order to minimize the stratification of gas within the space and its potentially more rapid leakage. | NR | This is a statement not a requirement. |
| **DRY POWDER AND CHEMICAL EXTINGUISHING SYSTEMS** | | | |
| II.82. | Dry powder and chemical fire suppression systems consist of a stored quantity of powder or chemical suppression agent, a source of compressed gas propellant, an associated distribution network, discharge nozzles and provisions for detection and/or actuation. The systems can be either manually operated at the location of the hazard, or remotely or automatically actuated by a detection system. These systems are usually used to protect against flammable liquid fires and certain fires involving electrical equipment. These extinguishing agents should not be used on sensitive electrical equipment since they generally leave a corrosive residue. | COM | Chemical extinguishing systems are not used on sensitive electrical equipment. |
| II.83. | The type of powder or chemical agent selected should be compatible with the combustible material and/or the hazard. Special powders should be used to fight metal fires. | COM | The FPS is designed to comply with NFPA 10, “Standard for Portable Fire Extinguishers” [11] for portable fire extinguishers. |
| II.84. | Careful consideration should be given to the use of dry powder systems in possibly contaminated areas, since decontamination following their discharge could be rendered more difficult owing to residues of contaminated powder. The consequential clogging of filters (e.g. ventilation system filters) should also be taken into account. | COM | Dry chemical fire extinguishers are not used in possibly contaminated areas due to cleanup and contamination concerns. A dry chemical portable fire extinguishers are provided only in fire zone 1270 AF 12701. See DCD [2] Section 9A.3.1.1.17. |
| II.85. | The possible adverse effects of using dry powders in conjunction with other extinguishing systems such as foam systems should be considered; some combinations should not be used. | COM | The effects of using dry chemical fire extinguishers have been evaluated. |
| II.86. | Since dry powders do not provide cooling or an inerting atmosphere and only minimally secure the hazard, precautions should be taken to prevent or to reduce the possibility of re‑ignition of a fire. | COM | Additional protective measures have been provided to prevent re-ignition of a fire. |
| II.87. | Dry powder systems are difficult to maintain. Precautions should be taken to ensure that the powder does not compact in its storage container and that the nozzles do not become blocked during discharge. | OR | The Owner shall be responsible for ensuring this requirement is met during operation. |
| **PORTABLE AND MOBILE FIRE EXTINGUISHING EQUIPMENT** | | | |
| II.88. | Portable and mobile fire extinguishers of a type and size suitable for the hazards being protected against should be provided for use, as necessary, in manual firefighting by plant personnel and external firefighters. The entire plant should be equipped with a sufficient number of portable and mobile extinguishers of the appropriate type as well as spares or facilities for recharging. | COM  OR | Portable fire extinguishers are accessible throughout the plant. The FPS is designed to comply with NFPA 10 [13] for portable fire extinguishers.  The Owner shall be responsible for ensuring this requirement is met during operation. |
| II.89. | Fire extinguishers should be placed close to the locations of fire hoses and along the access routes and escape routes for fire compartments. All fire extinguisher locations should be clearly indicated. | COM  OR | The FPS is designed to comply with NFPA 10, “Standard for Portable Fire Extinguishers” [13] for portable fire extinguishers. The Owner is responsible for ensuring this requirement is met during operation. |
| II.90. | Consideration should be given to the possible adverse consequences of the use of extinguishers, such as cleaning up after the use of dry powder extinguishers. | COM  N/A | See Section 9.5 and Appendix 9A to the AP1000 plant DCD [2]. Consequences regarding the use of extinguishers have been considered. Dry chemical fire extinguishers are not used in possibly contaminated areas due to cleanup and contamination concerns. |
| II.91. | In plant areas with potential hazards due to flammable liquids, foam concentrate for firefighting and portable equipment that is suitable for the hazard should be readily available. | COM  OR | The FPS detects fires and provides the capability to extinguish them using fixed automatic and manual suppression systems, manual hose streams, and/or portable firefighting equipment. The FPS is designed to comply with NFPA 10 [13] for portable fire extinguishers.  The Owner shall be responsible for ensuring this requirement is met during operation. |
| II.92. | Portable and mobile extinguishers filled with water or foam solution, or other extinguishing agents with a neutron moderating capability, should not be used in locations where nuclear fuel is stored, handled or passes in transit unless an assessment of the criticality hazard has demonstrated that it is safe to do so. | OR | The Owner shall be responsible for ensuring this requirement is met during operation. |
| **PROVISIONS FOR MANUAL FIREFIGHTING** | | | |
| II.93. | Manual firefighting forms an important part of the defence in depth strategy for firefighting. The extent of reliance on on‑site and off‑site fire services should be established at the design stage. The location of the site and the response time of any off‑site fire service will affect the necessary level of provision for manual firefighting. Recommendations on manual firefighting capabilities are provided in NS‑G‑2.1 [23]. | OR | The availability of fire protection and firefighting systems/equipment is discussed in DCD [2] Section 9.5.1 and Appendix 9A (Reference 23). The staffing, training, and procedures for offsite/onsite firefighting by the fire brigade are to be developed by the Owner. |
| II.94. | The design of the plant should allow access by fire teams and off‑site fire services using heavy vehicles. | COM | Adequate infrastructure will be provided to permit the use of heavy vehicles. See DCD [2] Section 1.2.2. |
| II.95. | Suitable emergency lighting and communications equipment should be provided for all fire compartments to support the operation of manual firefighting activities. These should be functional at all times and should be provided with non‑interruptible emergency power supplies. | COM | To achieve the required high degree of fire safety, and to satisfy fire protection objectives, the AP1000 plant is designed to provide emergency lighting and communications to facilitate safe shutdown following a fire.  The AP1000 normal and emergency lighting system is designed to provide illumination levels required for the safe performance of plant operation under normal and emergency conditions. |
| II.96. | A wired emergency communication system with a reliable power supply should be installed at preselected stations: see SSG‑62 [12]. | COM | Fixed emergency communications, independent of the normal plant communication system, are installed at preselected stations. |
| II.97. | Alternative communication equipment such as two way radios should be provided in the control room and at selected locations throughout the plant. In addition, portable two way radios should be provided for the firefighting team. | OR | The Owner shall be responsible for meeting this requirement. |
| II.98. | Self‑contained breathing apparatus, including spare cylinders and a facility for recharging, should be provided at appropriate locations for use by suitably trained personnel. | COM  OR | The compressed and instrument air system (CAS) provides a self-contained breathing apparatus (SCBA) refill station package. The SCBAs shall be the responsibility of the Owner. |
| II.99. | Arrangements for plant equipment and for its storage in the plant should be designed to facilitate access for firefighting, as far as practicable. | COM | The AP1000 plant arrangement is designed to access firefighting operations. |
| II.100. | Detailed firefighting strategies should be developed for locations containing items important to safety. | OR | Westinghouse has performed the FPS design and fire protection analysis in accordance with the Westinghouse Quality Management System. The Owner shall be responsible for implementing the fire protection program. |
| **PROVISIONS FOR VENTING SMOKE AND HEAT** | | | |
| II.101. | An assessment should be carried out to determine the need for venting smoke and heat, including the need for dedicated smoke and heat extraction systems, to confine the products of combustion and prevent the spread of smoke, to reduce temperatures and to facilitate manual firefighting. | COM | Some examples of heat/smoke control are discussed in DCD Section 9.4 [2] and the fire protection analysis of individual fire areas/zones.  The fire protection analysis verifies that the ventilation system for the fire area does not contribute to the spread of fire or smoke. |
| II.102. | In the design of a smoke and heat extraction system, the following criteria should be taken into account: fire load, smoke propagation behaviour, visibility, toxicity, fire service access, the type of fixed fire extinguishing systems used and radiological aspects. | COM | These items have been considered. Smoke and heat venting capability is provided as described in DCD [2] Appendix 9A. Some examples of heat/smoke control are discussed in DCD [2] Section 9.4 and the fire protection analysis of individual fire areas/zones. |
| II.103. | The necessary capability of the smoke and heat extraction system should be determined from assessments of the smoke and heat released from the postulated fire for the fire compartment. The following locations should have provisions for venting smoke and heat:  (a) Areas containing a high fire load due to electrical cables;  (b) Areas containing a high fire load due to flammable liquids;  (c) Areas containing items important to safety (including safety features for design extension conditions) that are normally occupied by operating personnel (e.g. the main control room). | COM | Smoke and heat venting capability is provided as described in DCD [2] Appendix 9A. Some examples of heat/smoke control are discussed in DCD [2] Section 9.4 and the fire protection analysis of individual fire areas/zones. |

# SUMMARY AND CONCLUSIONS

## IDENTIFIED POTENTIAL RISKS TO BE ADDRESSED IN FUTURE PROJECT

Based on the assessment performed in Section 2 of this document, there are no significant obstacles for the AP1000 plant design to fulfill this assessed regulation from a physical design standpoint.

## NON-COMPLIANCES

There are no non-compliances identified based on the assessment.

# REFERENCES

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-64, IAEA, Vienna (2021).
2. APP-GW-GL-700, Rev. 19, “AP1000 Design Control Document,” Westinghouse Electric Company LLC. (Publicly available at: www.nrc.gov/docs/ML1117/ML11171A500.html).
3. Vogtle, Units 3 and 4, Rev. 11 to Updated Final Safety Analysis Report. NRC Accession Number Link: ML22179A145 (6462 page(s)). Date Released: Wednesday, June 29, 2022. (Publicly available at: https://www.nrc.gov/docs/ML2217/ML22179A145.html).
4. APP-GW-GL-022, Rev. 8, “Probabilistic Risk Assessment.”
5. NUREG-0800, U. S. Nuclear Regulatory Commission Standard Review Plan, Section 9.5.1, “Fire Protection Program,” Rev. 3, July 1981, including Branch Technical Position (BTP) CMEB 9.5-1, “Guidelines for Fire Protection for Nuclear Power Plants,” Revision 2, July 1981.
6. ANSI/ANS-56.11-1988, "Design Criteria for Protection against the Effects of Compartment Flooding in Light Water Reactor Plants."
7. APP-GW-GL-059, Rev. 2, “AP1000 Plant Design Comparison to IAEA Safety Standard No. SSR-2/1 - Safety of Nuclear Power Plants: Design.”
8. APP-GW-GL-100 Rev. 0, “API000 Conformance with Nuclear Regulatory Commission General Design Criteria.”
9. NPP\_NPP\_000065, Rev. 0, “Westinghouse AP1000 Nuclear Power Plant – Coping with Station Blackout.”
10. NPP\_NPP\_000067, Rev. 0, “Westinghouse AP1000 Nuclear Power Plant – Spent Fuel Pool Cooling).”
11. NPP\_NPP\_000072, Rev. 0, “Westinghouse AP1000 Nuclear Power Plant – Response to External Hazards.”
12. APP-GW-G0R-005, Rev. A, “Assessment of the AP1000 Plant to IAEA Specific Safety Guide No. SSG-30 "Safety Classification of Structures, Systems and Components In Nuclear Power Plants.”
13. National Fire Protection Association Codes and Standards:

* NFPA 10, “Standard for Portable Fire Extinguishers,” 2013.
* NFPA 13, “Standard for the Installation of Sprinkler Systems,” 2013.
* NFPA 14, “Standard for the Installation of Standpipe and Hose Systems,” 2013.
* NFPA 15, “Standard for Water Spray Fixed Systems for Fire Protection,” 2012.
* NFPA 20, “Standard for the Installation of Stationary Pumps for Fire Protection,” 2013.
* NFPA 22, “Standard for Water Tanks for Private Fire Protection,” 2013.
* NFPA 24, “Standard for Installation of Private Fire Service Mains and Their Appurtenances,” 2013.
* NFPA 30, “Flammable and Combustible Liquids Code,” 2015.
* NFPA 50A, “Standard for Gaseous Hydrogen Systems at Consumer Sites,” 1999.
* NFPA 50B, “Standard for Liquefied Hydrogen Systems at Consumer Sites,” 1999.
* NFPA 72, “National Fire Alarm and Signaling Code,” 2013.
* NFPA 90A, “Standard for Installation of Air Conditioning and Ventilation Systems,” 1999.
* NFPA 92A, “Recommended Practice for Smoke Control Systems,” 2000.
* NFPA 251, “Standard Methods of Tests of Fire Resistance of Building Construction and Materials,” 2006.
* NFPA 497, “Recommended Practice for the Classification of Flammable Liquids, Gases, or Vapors and of Hazardous (Classified) Locations for Electrical Installations in Chemical Process Areas;” 2012.
* NFPA 780, “Standard for the Installation of Lightning Protection Systems,” 2014.
* NFPA 804, “Standard for Fire Protection for Advanced Light Water Reactor Electric Generating Plants,” 2010.
* NFPA 1964, “Spray Nozzles,” 2013.

1. Westinghouse Document WCAP-15871, Rev. 1, “AP1000 Assessment Against NFPA 804,” December 2002.
2. IEEE Std. 1202 – 1991, “IEEE Standard for Flame Testing of Cables for Use in Cable Tray in Industrial and Commercial Occupancies,” Institute of Electrical and Electronics Engineers, 1991.
3. IEEE Std. 383-1974, “IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1974.
4. Regulatory Guide 1.91, Rev. 2, “Evaluation of Explosions Postulated to Occur on Transportation Routes Near Nuclear Power Plant Sites,” U. S. Nuclear Regulatory Commission, 1978.
5. ANSI/ANS-58.2-1988, “Design Bases for Protection of Light Water Nuclear Power Plants Against Effects of Postulated Pipe Rupture.”
6. Westinghouse Report APP-GW-N1-001, Rev. 0, “Pipe Rupture Protection Design Criteria for AP1000”, 9 September 2002.
7. NUREG-1061, Volume 3, Report of the U. S. Nuclear Regulatory Commission Piping Review Committee, Evaluation of Potential for Pipe Breaks, November 1984.
8. Standard Review Plan 3.6.3, “Leak Before Break Evaluation Procedures,” Federal Register, Volume 52, Number 167, Friday, August 28, 1987; Notice (Public Comment Solicited), pp. 32626-32633.
9. Biggs, J. M., Introduction to Structural Dynamics, McGraw-Hill Book Company, New York, 1964.
10. "Evaluation of Seals for Mechanical Penetrations of Containment Buildings," NUREG/CR-5096 SAND88-7016.
11. APP-GW-G0R-013, Rev. A, “Assessment of the AP1000 Plant to IAEA Specific Safety Guide No. SSG-63 "Design of Fuel Handling and Storage Systems for Nuclear Power Plant.”
12. Not used.
13. APP-GW-A1-103, Rev. 0, “Engineering Area Management Room Review Guideline for Egress and Life Safety.”
14. APP-GW-A2R-001, Rev. 0, “AP1000 Means of Egress Study.”
15. APP-G1-A2R-001, Rev. 0, “AP1000 Annex, Radwaste, and Diesel Generator Building Architectural Means of Egress Study.”
16. Regulatory Guide 1.75, Revision 2, “Physical Independence of Electric Systems,” U. S. Nuclear Regulatory Commission”, 1976.
17. APP-GW-G0R-007, Rev. A, “Assessment of the AP1000 Plant to IAEA Specific Safety Guide No. SSG-39 "Design of Instrumentation and Control Systems for Nuclear Power Plants."