Page 2 of 319

BGP-GW-GL-203  
Revision A

Assessment of the AP1000 Plant for the Bulgarian Regulation Related to Ensuring Safety 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 | Hannu Tuulensuu  Sergio Díaz | Initial Document 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 9](#_Toc152234612)

[1.1 OVERVIEW AND PURPOSE OF DOCUMENT 9](#_Toc152234613)

[1.2 STANDARD AP1000 PLANT AS BASIS FOR THE ASSESSMENT 9](#_Toc152234614)

[1.2.1 OVERVIEW OF THE AP1000 PLANT LICENSING DOCUMENTATION 10](#_Toc152234615)

[1.3 APPLICATION OF THE REGULATION TO THE AP1000 PLANT 11](#_Toc152234616)

[1.3.1 Application of the Regulation of Ensuring the Safety of Nuclear Power Plants for Site Selection for an AP1000 13](#_Toc152234617)

[2 AP1000 PLANT DESCRIPTION APPLICABLE TO THE REGULATION 15](#_Toc152234618)

[2.1.1 Plant Description Overview 15](#_Toc152234619)

[2.1.2 Passive Safety Systems 16](#_Toc152234620)

[2.1.3 Defense in Depth Systems 18](#_Toc152234621)

[2.1.4 Regulatory Treatment of Non-Safety-Related AP1000 Plant Class D SSCs with Importance to Safety 19](#_Toc152234622)

[2.1.5 Robust Protection 20](#_Toc152234623)

[2.1.6 Resiliency to Extreme External Hazards and Post-Fukushima Lessons Learned. 21](#_Toc152234624)

[3 REGULATION RISK ASSEMENT CATEGORIES 26](#_Toc152234625)

[4 DETAILED ASSESSMENT OF REGULATION CLAUSES AND REQUIREMENTS 27](#_Toc152234628)

[4.1 REGULATION ARTICLES/SUBARTICLES Compliance assessment Categories 27](#_Toc152234629)

[4.2 CHAPTER I - GENERAL PROVISIONS 28](#_Toc152234630)

[4.3 CHAPTER 3 - SITE CHARACTERISTICS 39](#_Toc152234631)

[4.3.1 Section I: General Requirements 39](#_Toc152234632)

[4.3.2 Section II: Studies of Natural and Human Induced Factors for Site Selection 44](#_Toc152234633)

[4.4 CHAPTER 4 - DEFENCE IN DEPTH AND DESIGN BASIS 57](#_Toc152234634)

[4.4.1 Section I: Defence in Depth Implementation in the Design 57](#_Toc152234635)

[4.4.2 Section II: Design Basis 65](#_Toc152234636)

[4.5 CHAPTER 5 - SAFETY ASSESSMENTS 96](#_Toc152234637)

[4.5.1 Section I: General Requirements 96](#_Toc152234638)

[4.5.2 Section II: Deterministic Safety Analysis 117](#_Toc152234639)

[4.5.3 Section III: Probabilistic Safety Analysis 127](#_Toc152234640)

[4.5.4 Section IV: Analysis of External Events and Hazards 133](#_Toc152234641)

[4.6 CHAPTER 6 – REQUIREMENTS FOR DESIGN OF NPP AND PLANT SYSTEMS 149](#_Toc152234642)

[4.6.1 Section I: General Requirements 149](#_Toc152234643)

[4.6.2 Section II: Reactor Core Design and Features 160](#_Toc152234644)

[4.6.3 Section III: Reactor Shutdown Systems 166](#_Toc152234645)

[4.6.4 Section IV: Instrumentation and Control Systems 172](#_Toc152234646)

[4.6.5 Section V: Reactor Coolant System 183](#_Toc152234647)

[4.6.6 Section VI: System for Core Cooling and Heat Transfer to an Ultimate Heat Sink 191](#_Toc152234648)

[4.6.7 Section VII: Structures and Systems Performing Confinement Safety Function 196](#_Toc152234649)

[4.6.8 Section VIII: Supporting Safety Systems 209](#_Toc152234650)

[4.6.9 Section IX: Other SSCs Important to Safety 215](#_Toc152234651)

[4.6.10 Section X: District Heating System 218](#_Toc152234652)

[4.6.11 Section XI: Radioactive Waste Management 219](#_Toc152234653)

[4.6.12 Section XII: Handling and Storage of Nuclear Fuel 223](#_Toc152234654)

[4.6.13 Section XIII: Radiation Protection 227](#_Toc152234655)

[4.7 CHAPTER 7 – CONSTRUCTION AND COMMISSIONING 234](#_Toc152234656)

[4.7.1 Section I: General Requirements 234](#_Toc152234657)

[4.7.2 Section II: Commissioning Program 239](#_Toc152234658)

[4.8 CHAPTER 8 – OPERATIONS 245](#_Toc152234659)

[4.8.1 Section I: Operational Safety Management 245](#_Toc152234660)

[4.8.2 Section II: Conduct of Operations 276](#_Toc152234661)

[4.8.3 Section III: Maintenance, Tests, Surveillance, and Inspections. Ageing Management 290](#_Toc152234662)

[4.8.4 Section IV: Radiation Protection During Operations 302](#_Toc152234663)

[5 SUMMARY AND CONCLUSIONS 311](#_Toc152234664)

[5.1 OVERALL HIGH LEVEL RISK ASSESSMENT 311](#_Toc152234665)

[5.2 IDENTIFIED POTENTIAL RISK TO BE ADDRESSED IN BULGARIA PROJECT 311](#_Toc152234666)

[6 REFERENCES 318](#_Toc152234667)

LIST OF ACRONYMS AND ABBREVIATIONS

|  |  |
| --- | --- |
| AC | Alternating current |
| ADS | Automatic Depressurization System |
| ALARA | As Low As Reasonably Achievable |
| ANSI | American National Standards Institute |
| AOP | Abnormal Operating Procedure |
| ARP | Alarm Response Procedures |
| ASME | American Society of Mechanical Engineers |
| ASUNE | Bulgarian Act on the Safe Use of Nuclear Energy. Also known as SUNEA |
| ATWS | Anticipated Transient Without Scram |
| BDB | Beyond Design Basis |
| BGP | Bulgaria Standard for AP1000 plants |
| BNRA | Bulgarian Nuclear Regulatory Agency |
| CCI | Concrete-Concrete Interaction |
| CCS | Component Cooling Water System |
| CDF | core damage frequency |
| CFR | Code of Federal Regulations |
| CIV | Containment Isolation Valve |
| CMT | core makeup tank |
| CNS | Containment System |
| COM | Compliant |
| COM-B | Compliant with planned update for Bulgaria Units |
| COL | Combined Operating License |
| CVS | Chemical and Volume Control System |
| CWO | Compliant with Objective |
| DAS | Diverse Actuation System |
| DBA | Design basis accident |
| DBE | Design Basis Event |
| DC | Direct Current |
| DCD | Design Control Document |
| DEC | Design Extension Condition |
| DiD | Defense-in-D |
| DOS | Standby Diesel Fuel Oil System |
| D-RAP | Design Reliability Assurance Program |
| DSFSF | Dry Spent Fuel Storage Facility |
| EAB | exclusion area boundary |
| ECCS | Emergency Core Cooling System |
| ECS | Main AC Power System |
| EDS | Non Class 1E DC and UPS System |
| EMC | ElectroMagnetic Compatibility |
| ENSREG | European Nuclear Safety Regulators Group |
| EOP | Emergency Operating Procedures |
| EPRI | Electric Power Research Institute |
| EQ | Equipment Qualification |
| EU | European Union |
| FEED | Front End Engineering Development |
| FHS | Fuel Handling and Refueling System |
| FPS | Fire Protection System |
| FWS | Main and Startup Feedwater System |
| GDC | General Design Criterion |
| GSI | Generic Safety Issue |
| HX | heat exchanger |
| IAEA | International Atomic Energy Agency |
| IEEE | Institute of Electrical Engineers |
| IDS | Class 1E DC and UPS System |
| INPO | Institute of Nuclear Power Operations |
| IIS | Incore Instrumentation System |
| IRWST | In-containment Refueling Water Storage Tank |
| IVR | In-Vessel Retention |
| KNPP | Kozloduy Nuclear Power Plant |
| KNPP-NB | KNPP Newbuilds. A public limited company registered in the Republic of Bulgaria |
| KZ7 | Kozloduy Unit 7 (Part of Bulgaria Standard BGP) |
| KZ8 | Kozloduy Unit 8 (Part of Bulgaria Standard BGP) |
| KZG | Kozloduy Site AP1000s (Part of Bulgaria Standard BGP) |
| LBB | Leak-Before-Break |
| LERF | Large Early Release Frequency |
| LOCA | Loss Of Coolant Accident |
| LPZ | Low Population Zone |
| LRF | large release frequency |
| MAAP | Modular Accident Analysis Program |
| MCR | Main Control Room |
| MR | Maintenance Rule |
| MSIV | Main Steam Isolation Valve |
| MSLB | Main Steam Line Break |
| N/A | Not Applicable |
| NAS | Not Assessable |
| NDF | Bulgarian National disposal facility for low and intermediate level RAW |
| NOC | Non-Compliant |
| NOP | Normal Operating Procedure |
| NR | Not a Requirement |
| NRC | Nuclear Regulatory Commission |
| OR | Owner Requirement |
| PAR | Passive Autocatalytic Recombiner |
| PCCWST | Passive Containment Cooling Water Storage Tank |
| PCS | Passive Containment Cooling System |
| PIE | Postulated Initiating Event |
| PLS | Plant Control System |
| PMS | Protection and Safety Monitoring System |
| PRA | Probabilistic Risk Assessment |
| PRHR | Passive Residual Heat Removal |
| PRHR HX | Passive Residual Heat Removal Heat Exchanger |
| PSA | Probabilistic Safety Assessment |
| PSAR | Preliminary Safety Analysis Report |
| PXS | Passive Core Cooling System |
| PWR | Pressurized Water Reactor |
| QMS | Quality Management System |
| RAM | Risk-Oriented Accident Analysis |
| RAW | Radioactive Waste |
| RCCA | Rod Cluster Control Assembly |
| RCP | Reactor Coolant Pump |
| RCS | Reactor Coolant System |
| RG | Regulatory Guide |
| RHWG | Reactor Harmonization Working Group |
| RMS | Radiation Monitoring System |
| RNS | Residual Heat Removal System |
| RSP | Remote Shutdown Panel |
| RSR | Remote Shutdown Room |
| RSW | Remote Shutdown Workstation |
| RTNSS | Regulatory Treatment of Non-Safety Systems |
| SAMG | Severe Accident Management Guidelines |
| SERAW | Bulgarian State Enterprise for “Radioactive Waste” |
| SFP | Spent Fuel Pool |
| SFS | Spent Fuel Pool Cooling System |
| SGS | Steam Generator System |
| SGTR | Steam Generator Tube Rupture |
| SSC | Structures, Systems, and Components |
| SUNEA | Bulgarian Safe Use of Nuclear Energy Act. Also known as (ASUNE) |
| TEDE | Total Effective Dose Equivalent |
| TSC | Technical Support Center |
| UK | United Kingdom |
| US | United States |
| VAS | Radiologically Controlled Area Ventilation System |
| VBS | Nuclear Island Nonradioactive Ventilation System |
| VZS | diesel generator building heating and ventilation system |
| WENRA | Western European Nuclear Regulators’ Association |
| WSF | Wet Spent Fuel Storage Facility |
| WWER | Water Cooled Water Moderated Energy Reactor. Russian Design PWRs. |
| ZOS | Onsite Standby Power System |

# INTRODUCTION

## OVERVIEW AND PURPOSE OF DOCUMENT

This document provides a compliance assessment of the standard AP1000 plant design to the following Bulgaria regulation:

* Regulation on Ensuring the Safety of Nuclear Power Plants [1].

The regulation of [1] is herein referred to as the “Safety Regulation”.

This document is performed as part of the 2023 Front End Engineering and Design Work Agreement.

The articles of this Regulation have been provided as contract Input I.02.01 containing the “Applicable regulations, guides, codes and standards that are planned to be invoked by KNPP Newbuilds, translated into English” by the Letter **L.KNP\_WEC\_230003** [1] in which KNPP Newbuilds has provided the list of 26 documents to be reviewed in this FEED Task 2.

The purpose of this task during FEED is the identification of potential design risks and priorities for assessment work to be performed in a future project phase.

## 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” [3], herein referred to the as the Design Control Document (DCD [3]). 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 AP1000 Units design, which have publicly available information of their FSAR available in reference [3]. There are design and licensing updates incorporated into the Vogtle Units 3 and 4 design that have occurred since the issuance of the DCD [3]. However, the DCD [3] 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 the project related with Bulgaria regulations and invoked regulations, guides, codes and standards, that could potentially be used in the project at a later stage.

During the risk assessment process performed in this document, the current Vogtle 3 and 4 AP1000 plant design and licensing basis has been reviewed within the context of the Bulgaria regulation requirements.

If there has been a significant deviation from the design, methodology, or safety analysis approach since the time of the DCD [3] documentation that would impact compliance/risks with the Bulgaria regulation, this would be identified in the assessment of that particular article of the regulation.

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 [3]. 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 [3] and because it adequately demonstrates the PRA methodology and PRA basis for the overall AP1000 plant design. For the Bulgaria AP1000 plant project, the updated Vogtle Unit 3&4 PRA will be the basis for the future PRA as one of the Vogtle AP1000 units will be the reference plant.

This High Level Risk Assessment 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 Votgle Reference Plant 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 design and licensing basis and incorporation of design changes implemented for the Bulgaria AP1000 plant project and any new analyses that may need to be performed for the Bulgaria AP1000 to address final compliance with the Regulation [1].

### OVERVIEW OF THE AP1000 PLANT LICENSING DOCUMENTATION

Westinghouse as a nuclear technology vendor has developed multiple nuclear power plant designs. AP600 and AP1000 plant designs were documented accordingly to binding regulations and guidance’s in the United States (US). Nuclear Regulatory Commission (NRC) issued multiple guidance’s which are the basis for the Design Control Document (DCD) that is used in the licensing approach under 10 CFR 52. One of them is Regulatory Guide (RG) 1.70 “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants” which was initially published February 1972 and last revised November 1978. RG 1.70 provides detailed guidance in preparing applications for construction permits and operating licenses for new nuclear power plants. Content of the DCD also follows the NUREG-0800 “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” that is dividing the structure of the DCD into 19 chapters:

* + - * Cover, Table of Contents, and Introduction
      * Chapter 1, Introduction and Interfaces
      * Chapter 2, Sites Characteristics and Site Parameters
      * Chapter 3, Design of Structures, Components, Equipment, and Systems
      * Chapter 4, Reactor
      * Chapter 5, Reactor Coolant System and Connected Systems
      * Chapter 6, Engineered Safety Features
      * Chapter 7, Instrumentation and Controls
      * Chapter 8, Electric Power
      * Chapter 9, Auxiliary Systems
      * Chapter 10, Steam and Power Conversion System
      * Chapter 11, Radioactive Waste Management
      * Chapter 12, Radiation Protection
      * Chapter 13, Conduct of Operations
      * Chapter 14, Initial Test Program and ITAAC-Design Certification
      * Chapter 15, Transient and Accident Analysis
      * Chapter 16, Technical Specifications
      * Chapter 17, Quality Assurance
      * Chapter 18, Human Factors Engineering
      * Chapter 19, Probabilistic Risk Assessment/ Severe Accidents

In the United States (US) referral to the DCD combined with an Early Site Permit (ESP) can be used under 10 CFR 52 regulation to license a nuclear power plant. These documents with additional information (ex. site-specific, procedures) allow the licensee to obtain a Combined Operating License (COL) which grants permission to start the construction of the Nuclear Power Plant. The DCD with these additional information is used initially as the Preliminary Safety Analysis Report (PSAR) and with future modifications as the Final Safety Analysis Report (FSAR) or the Updated Final Safety Analysis Report (UFSAR). The SAR document is delivered to the Regulatory Body (in United States – NRC) and its role is to demonstrate in front of the Regulatory Body that the plant is maintained within the binding limits, procedures and regulations.

The AP1000 plant DCD [2] has been developed to meet the licensing basis documentation requirements set by the United States Nuclear Regulatory Commission, however it can be used as an input document in other countries licensing process for AP1000 plant designs. The DCD content covers a significant amount of information needed to prepare the Safety Analysis Reports which are compulsory to prepare in most countries.

Note that in the DCD [2] the terms “Combined License Applicant” and “Combined License Information” are used. This terminology is used in the US licensing basis and refers to the responsibility of the Licensee/Owner to fulfill the specific Licensee/Owner information in the development of the plant specific UFSAR from the standard AP1000 plant DCD information. Sections of the DCD identified as “Combined License Information” are the responsibility of the Licensee/Owner of AP1000 units to provide the content for the safety analysis report.

The Vogtle Unit 3 and 4 UFSAR [3] includes the “Combined License Information” that was required for the Owner/Licensee to provide to fulfill the UFSAR. This provides an example of the type of information to be generated by the Owner/Licensee.

## APPLICATION OF THE REGULATION TO THE AP1000 PLANT

Safety Regulation defines the basic criteria and rules of nuclear safety and radiological protection, as well as the administrative provisions and the technical requirements for ensuring safety during the lifecycle of the NPP.

The Regulation on Ensuring the Safety of Nuclear Power Plants [1] is divided into the following section and subsections:

* Chapter 1: General Provisions
* Chapter 2: Operating Organisation
  + Section I: General Requirements
  + Section II: Management System
* Chapter 3: Site Characteristics
  + Section I: General Requirements
  + Section II: Studies of Natural and Human Induced Factors for Site Selection
* Chapter 4: Defense in Depth and Design Basis
  + Section I: Defense in Depth Implementation in the Design
  + Section II: Design Basis
* Chapter 5: Safety Assessment
  + Section I: General Requirements
  + Section II: Deterministic Safety Analysis
  + Section III: Probabilistic Safety Analysis
  + Section IV: Analysis of External Events and Hazards
* Chapter 6: Requirements for Design of NPP and Plant Systems
  + Section I: General Requirements to NPP
  + Section II: Reactor Core Design and Features
  + Section III: Reactor Shutdown Systems
  + Section IV: Instrumentation and Control Systems
  + Section V: Reactor Coolant System
  + Section IV: Systems for Core Cooling and Heat Transfer to an Ultimate Heat Sink
  + Section VII: Structures and System Performing Confinement Safety Function
  + Section VIII: Supporting Safety Systems
  + Section IX: Other SSCs Important for Safety
  + Section X: District Heating System
  + Section XI: Radioactive Waste Management
  + Section XII: Handling and Storage of Nuclear Fuel
  + Section XIII: Radiation Protection
* Chapter 7: Construction and Commissioning
  + Section I: General Requirements
  + Section II: Commissioning Programme
* Chapter 8: Operations
  + Section I: Operational Safety Management
  + Section II: Conduct of Operations
  + Section III: Maintenance, Tests, Surveillance, and Inspections. Ageing Management
  + Section IV: Radiation Protection During Operations

The following chapters or sections are excluded from detailed assessment as they have no requirements regarding the design of the New Nuclear Power Units.

* Chapter 2: Operating Organization
* Chapter 5: Safety Assessment
  + Section V: Periodic Safety Review
* Chapter 8: Operations
  + Section V: Personnel Qualification and Training
  + Section VI: Management of Safety Related Documentation
  + Section VII: Preparation for Decommissioning

### Application of the Regulation of Ensuring the Safety of Nuclear Power Plants for Site Selection for an AP1000

**Kozloduy Site Reactors:**

In 1974, Bulgaria's first commercial nuclear reactor was commissioned at Kozloduy Nuclear Power Plant (KNPP). KNPP Units 1 through 4 started commercial operation from 1974 to 1982. KNPP Units 1-4 were reactor-type WWER-440, model В-230 (Units 1 and 2) and advanced model V-230 (Units 3 and 4). KNPP Units 1 & 2 and KNPP Units 3 & 4 were shut down in 2002 and 2006, respectively, prior to the expiry of their design life in pursuance of commitments undertaken by the Republic of Bulgaria during its accession into the European Union (EU). With decrees of the Council of Ministers, 20.12.2008 for Units 1 and 2, and decree of 19.12.2012 for Units 3 and 4, these power units were declared management of radioactive waste (RAW) facilities and were transferred to the Radioactive Waste State Enterprise (SERAW). In 2014 and 2016, the Bulgarian Nuclear Regulatory Agency (BRNA) issued decommissioning licences for Units 1 & 2 and Units 3 & 4, respectively.

There are currently two operating units at KNPP – Units 5 and 6. These units are WWER-1000 reactor-type, model B 320, pressurized water reactors with an installed electrical capacity of 2000 MW. Units 5 and 6 were commissioned in 1987 and 1991, respectively.

In November 2017 and October 2019, the BNRA renewed the operating licences for 10 years based on Periodic Safety Reviews (PSRs). Since 2019 and 2018, respectively, Units 5 and 6 have been operating at an upgraded thermal power level of 104% (3120 MW).

The KNPP site has two spent fuel storage facilities – the Wet Spent Fuel Storage Facility (WSF) and Dry Spent Fuel Storage Facility (DSFSF).

In 2012, the project company “Kozloduy NPP - New Build” EAD (KNPP-NB) was established. KNPP-NB is leading the effort to design, license, construct, and commission new nuclear capacities in the KNPP area. Therefore, KNPP-NB started the construction licensing procedure for the new nuclear facility by applying for the permit that establishes the new nuclear facility location (i.e., site selection). This permit was approved in August 2013. As a result, Westinghouse developed a Feasibility Study (TD-WES-13-002) to evaluate possible construction of a new unit in accordance with the Terms of Reference (ToR) developed by KNNP-NB.

The BNRA Chairman (by Order No. AA-04-30) granted approval in 2020 for the siting of a nuclear power plant (Site 2) chosen by KNPP-NB. This site approval order was based on the Site Assessment, which considered the characteristics of the site and surrounding area . This application also included a Preliminary Safety Analysis Report (PSAR), which was developed by KNPP-NB.

**Site Approval Order**

The Site Approval Order (Order No. AA-04-30) was granted by the Chairman of the Nuclear Regulation Agency and permits KNPP-NB to build a nuclear power plant (at Site 2) with the location, boundaries, and characteristics according to the submitted documents. Approval is based on:

1. The documents required by the Ordinance on the Procedure for the Issuance of Licenses and Permits for the Safe Use of Nuclear Energy are attached to the application for issuing of an order for the approval of the selected site;

2. The conditions set out in the Site Selection Permit No. КН-3665/26.08.2013 issued by the Chairman of the Nuclear Regulation Agency (NRA) for the selection of the site have been met.

3. No factors have been identified to preclude the deployment of a nuclear power plant on the selected site.

4. It is foreseen to take into account at the design stage the phenomena and factors identified for the selected site, that require additional measures to be taken in order to limit their impact on the nuclear power plant.

5. The Preliminary Safety Analysis Report (PSAR) justifies the feasibility of the construction and subsequent safe operation of a nuclear power plant at the selected site.

6. The site selection was carried out in accordance with the legislation in force in the field of safe use of nuclear energy.

The findings under Items 1 to 6 are based on the results of the review and evaluation of the documents carried out at the BRNA, as well as the results of the external expertise carried out in the PSAR. Based on the Site Approval Order KNPP-NB has obligations related to monitoring, maintenance, and management of the site.

There are no AP1000 plant design requirements stated in the Site Approval Order.

**AP1000 Standard Design and Site Selection:**

Standard Design as Documented in DCD Chapter 2 defines the site-related parameters for which the AP1000 plant is designed. The site parameters are in DCD Table 2-1. The sections of DCD Chapter 2 follow the standard format (R.G. 1.70) and discuss how the specific parameters are used in the AP1000 design and how a US-based Combined License applicant is to demonstrate that the site meets the design parameters.

A preliminary assessment of the compatibility of the standard design with the Site and Site Approval Order Requirements is shown in reference [9]

# AP1000 PLANT DESCRIPTION APPLICABLE TO THE REGULATION

### Plant Description Overview

The aspects of the design related to the scope of this regulation are described in AP1000 DCD [2] Chapters 1-19.

The AP1000 plant is an 1100-MWe pressurized water reactor (PWR) with passive safety features and extensive plant simplifications that enhance construction, operation, maintenance, and safety. One of the key design approaches in the AP1000 plant is to use passive features to mitigate design basis accidents (DBAs). In addition to redundancy, these features incorporate diversity based on probabilistic risk assessment (PRA, also called Probabilistic Safety Assessment or PSA) insights. Active defense-in-depth (DiD) features provide investment protection, reduce the demands on the passive features and support the aggressive 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 US. 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 (e.g., EUR and Electric Power Research Institute [EPRI] Utility Requirements Document [URD]). Safety systems use natural driving forces such as pressurized gas, gravity flow, natural circulation flow, and convection. Safety systems do not use active components (such as pumps, fans or diesel generators) and are designed to function without safety-grade support systems (such as alternating current [AC] power; component cooling water; service water; 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.

The AP1000 plant is designed to meet U.S. NRC deterministic safety criteria and probabilistic safety criteria with large margins. Safety analyses have been completed and documented in the U.S. licensing documents reviewed by the U.S. NRC (the AP1000 plant DCD [2] and the design PRA [4]). The extensive AP600 plant testing program, which is applicable to the AP1000 plant design, verifies that the innovative plant features will perform as designed and analyzed. PRA results show a very low core damage frequency (CDF) and large release frequency (LRF), which meet the goals established for advanced reactor designs. For the design PRA [4], the AP1000 plant mean CDF for internal initiating events at power (at power internal events, excluding seismic, fire and flood events) is 2.41 E-07 events per year. The total CFD including internal initiating events, internal flood, fires, and shutdown conditions is 5.09E-07 [4]. For the design PRA [4], the LRF for at power internal events (excluding seismic, fire, and flood events) is 1.95E-08 events per year. The LRF for at power internal events including internal flood, fire, and shutdown conditions) is 5.94E-08. This very low risk is a result of the AP1000 plant safety design features (simple passive safety features and active DiD features) as well as the use of PRA throughout the design process starting with the initial design phase. In addition, the AP1000 plant has carefully evaluated and addressed severe accident phenomenon. A key AP1000 plant design feature in dealing with a severe accident is the in-vessel retention (IVR) of a molten core. This feature provides a robust, reliable, and simple means of preventing a molten core from causing containment failure.

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

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

### Passive Safety Systems

The overarching AP1000 plant design principle with respect to nuclear safety is the use of simple, passive safety systems. These safety systems are dedicated to the mitigation of safety issues and are not required for normal operation. This approach is applicable to core cooling, core reactivity control, containment cooling, spent fuel cooling, DC power, and control room habitability.

**The AP1000 plant design employs the following passive safety functions:**

* Passive Core Cooling System (PXS): Passive residual heat removal and passive safety injection, as further described in DCD Section 6.3.
* Passive Containment Cooling System (PCS): Passive containment cooling by water evaporation and natural circulation of air; safety-related ultimate heat sink. See DCD Section 6.2.2.
* Containment: The containment vessel functions as the safety-related ultimate heat sink by transferring the heat associated with accident sources to the surrounding environment and it contains the release of radioactivity following postulated design basis accidents. See DCD Section 6.2.1.
* Main Control Room Emergency Habitability System (VES): The habitability system maintains an acceptable environment for continued operating staff occupancy. See DCD Section 6.4.
* Passive cooling of the Main Control Room (MCR) and rooms containing Instrumentation & Control systems by natural circulation to concrete walls/ceilings. See DCD Section 6.4.
* Containment Isolation: Provide containment isolation to preserve the integrity of the containment boundary. See DCD Section 6.2.3.
* Passive spent fuel pool cooling: Passive heat sink provides 72 hours of cooling. See DCD Section 9.3.1.
* Passive radiation removal from the containment atmosphere: Post accident safety-related fission product control is provided by natural removal processes inside containment, the containment boundary, and containment isolation system. See DCD Section 6.5.
* Passive containment hydrogen control: See DCD Section 6.2.4.
* Passive containment pH control by baskets of trisodium phosphate flooded by accident: See DCD Section 6.3.2.1.4.

**Passive safety functions are supported by the following:**

* Class 1E DC and Uninterrupted Power Supply (IDS) – See DCD Chapter 8 for additional description.
* Protection and Safety Monitoring System (PMS) – See DCD Chapter 7 for additional description.
* Reactor Trip
* Safeguards actuation of PXS, PCS, and VES
* MCR Safety PMS Control/Display Panel (if Plant Control System (PLS) / Diverse Actuation System (DAS) inoperable)

The AP1000 plant safety-related equipment design includes adequate redundancy to satisfy the single failure criterion. No maintenance is performed on the safety-related equipment (AP1000 Class A, B, and C) necessary to mitigate design basis conditions when they might be required to operate, i.e. during power operation, as well as during the shutdown stages during which they might be required to operate.

The safety-related Class 1E DC power system (IDS) includes four independent divisions of battery systems. Any three of the four divisions can support the equipment needed to shut down the plant safely and maintain it in a safe shutdown condition. Divisions B and C have two battery banks each. One of these battery banks is sized to supply power to selected safety-related loads for at least 24 hours, and the other battery bank is sized to supply power to another smaller set of selected safety-related loads for at least 72 hours following a design basis event (including the loss of all AC power). For supplying power during the post-72 hour period following a DBA, provisions are made to connect an ancillary AC generator to the Class 1E voltage regulating transformers (Divisions B and C only). This powers the Class 1E post-accident monitoring systems, lighting in the MCR, and ventilation in the MCR and Divisions B and C I&C rooms.

### Defense in Depth Systems

When AC power is available, the AP1000 passive systems can be supplemented with simple, active DiD structures, systems, and components (SSCs). The active DiD systems use reliable and redundant active equipment, supported by the use of DiD standby diesel generators to facilitate their functions when offsite AC power is not available. These simple, active SSCs are optimized for their normal operating functions. The active systems provide investment protection and reduce the overall risk to the plant owner and the public by minimizing the demand on the passive safety features. While important to the safe operation of the plant, the active systems are not necessary for the safe shutdown of the reactor following a DBA.

In other words, typical active pressurized water reactors safety-related systems and safety‑related support systems exist as simplified, yet redundant, DiD systems. The DiD system design includes sufficient redundancy so that the most probable single failures cannot result in the loss of the DiD functions. For example, this is accomplished by including two 100 percent capacity trains for systems such as spent fuel pool cooling, normal residual heat removal, and startup feedwater.

The following DiD systems provide diverse means of maintaining nuclear safety:

* The startup feedwater (SFW) portion of the feedwater system (FWS) supplies feedwater to the steam generators and, together with the steam generator system (SGS), removes heat from the RCS during plant startup, hot standby, and shutdown conditions, and following events such as a loss of main feedwater. The SFW and the SGS are described in DCD Sections 10.4.9 and 10.3.
* The SGS provides decay heat removal capability during plant startup, hot standby, and shutdown operations by delivery of startup feedwater flow to the steam generator and venting of steam from the steam generators to the atmosphere via the power‑operated relief valves. The SGS is described in DCD Section 10.3.
* The chemical and volume control system (CVS) consists of two centrifugal makeup pumps providing makeup flow and long-term boration to the RCS. The CVS is described in DCD Section 9.3.6.
* The normal residual heat removal system (RNS) removes heat from the core and RCS and provides RCS low-temperature overpressure protection (LTOP) at reduced RCS pressure and temperature conditions during cooldown and shutdown operation. The RNS can also be aligned to provide cooling of the spent fuel pool (SFP). The RNS is described in DCD Section 5.4.7.
* The spent fuel pool cooling system (SFS) cools the SFP water to remove decay heat from the spent fuel. The SFS is described in DCD Section 9.1.3.
* The CCS is a closed-loop cooling system that transfers heat from the RNS, SFS, and CVS to support their DiD functions during fault conditions. The CCS is described in DCD Section 9.2.2.
* The SWS transfers heat from the CCS heat exchangers in the turbine building to the environment. The SWS is described in DCD Section 9.2.1.
* The non-Class 1E DC and uninterruptible power supply (UPS) system (EDS) provides continuous, reliable electric power to the DiD components above. The EDS is described in DCD Section 8.3.2.
* The onsite standby power system (ZOS) consists of two onsite DiD standby diesel generator units and support systems that provides onsite AC electrical power for the EDS functions. The ZOS is described in DCD Section 8.3.1.
* The standby diesel fuel oil system (DOS) supplies fuel to the onsite standby power diesel generators. The DOS is described in DCD Section 8.3.2.
* The plant control system (PLS) controls the DiD systems from the main control room (MCR) or remote shutdown workstation. The PLS is further described in DCD Section 7.7.1.
* The nuclear island nonradioactive ventilation system (VBS) provides HVAC to the MCR envelope to maintain MCR habitability even in the presence of accidental release of radioactivity and provides HVAC to Class 1E I&C rooms, Class 1E DC equipment rooms, and Class 1E battery rooms. The VBS is described in DCD Section 9.4.1.
* The diesel generator building heating and ventilation system (VZS) provides HVAC to the diesel generator building, and HVAC to the diesel oil transfer module enclosure to support operation of the onsite standby power system. The VZS is described in DCD Section 9.4.10.
* The annex/auxiliary building nonradioactive heating and ventilation system (VXS) provides HVAC to the electrical switchgear rooms that contain the diesel bus switchgear and of the equipment room that contains the switchgear room air-handling units. The VXS is described in DCD Section 9.4.2.
* The central chilled water (VWS) provides chilled water to support the VBS, to support the cooling functions of the compartment unit coolers for the CVS and RNS pumps. The VWS is described in DCD Section 9.2.7.

In addition to those DiD systems performing prevention and mitigation DiD functions, defined ancillary equipment performs post-72 hours DiD functions. The passive safety systems include sufficient consumables (electric power supply via batteries or water supply) for 72 hours after the initiating event. Post-72 hours, there are several ways to maintain the safety functions: either the post-72 hours DiD systems can be used to supply consumables for four additional days or it is possible to perform prepared manual actions using mobile equipment and safety-related connections.

### Regulatory Treatment of Non-Safety-Related AP1000 Plant Class D SSCs with Importance to Safety

The regulatory treatment of the safety importance of AP1000 Class D SSCs has a significant effect on both the design and licensing of the plant. For the AP1000 plant design, the active systems are designated as non-safety-related systems except for limited portions of the systems that provide safety-related isolation functions, such as containment isolation. However, some of the non-safety-related AP1000 plant active systems (not AP1000 Class A, B, or C) provide DiD functions and can supplement the capability of the safety-related passive systems. Thus, a process is defined to evaluate the importance of the non-safety-related systems and to maintain appropriate regulatory oversight, as necessary, of these active systems.

SECY-94-084 and SECY-95-132 describe the scope, criteria, and process used to determine regulatory treatment of non-safety systems (RTNSS) in the passive plant designs. The Advanced LWR (ALWR) Utility Requirements Document (URD) describes the process to be used by the designer to identify the SSCs that are risk-important, to specify the needed reliability/availability (R/A) missions of these SSCs, and to propose appropriate additional regulatory requirements commensurate with their R/A missions. An R/A mission is the set of requirements related to the performance, reliability, and availability of an SSC function that adequately ensures the accomplishment of its task, as defined by PRA or deterministic criteria.

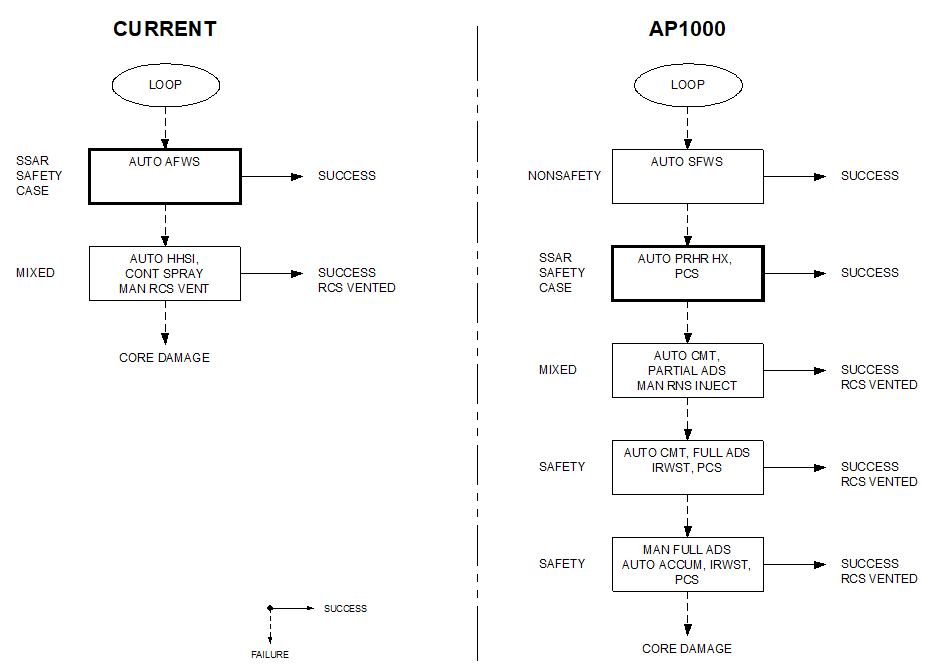
As a result of the assessment, appropriate additional regulatory oversight was determined for risk-important SSCs based on their R/A missions, such as an operational reliability assurance process, simplified technical specifications, and limiting conditions for operation to provide reasonable assurance that the missions can be met during operation.

### Robust Protection

In addition to the diversity provided by the active DiD systems, the AP1000 plant passive safety systems also provide functionally diverse methods to mitigate faults with frequencies above 10-3 per reactor year including anticipated transient without scram (ATWS) events and “frequent faults” with multiple failures.

Thus, the design includes more levels of defense and significant diversity for the more frequent initiating events. Robust protection for multiple / common mode failures are thus provided by the multiple levels of defense. This approach can be summarized as follows:

* Functional diversity and redundancy exists within the passive systems.
* Diversity exists between the passive and active systems.
* Redundancy exists within the active DiD systems.
* For example, for a loss of offsite power, the following lines of defense are available for core decay heat removal:
* The first line of defense is provided by the DiD systems: feedwater is provided to the steam generators by the startup portion of the FWS and steam is vented to the atmosphere by the SGS. Only one train of FWS is required to operator to mitigate the event.
* The second line of defense is provided by the passive core cooling system (PXS) and its passive residual heat removal heat exchanger (PRHR HX).
* In the event neither of the first two lines of defense operate as intended, automatic depressurization system (ADS) Stages 1-3 and use of RNS pumped injection (passive/active feed and bleed) are sufficient to mitigate the event.
* Finally, passive feed and bleed using the ADS valves (Stages 1-4) and the passive core cooling system safety injection sources could be used.
* This line of defense is illustrated in Figure 1. The figure illustrates the additional layers of defense the AP1000 plant design provides in comparison to a typical active pressurized water reactor (PWR).



**Figure 1: AP1000 Plant Lines of Defense for a Loss of Offsite Power Event**

### Resiliency to Extreme External Hazards and Post-Fukushima Lessons Learned.

Since its inception, the AP1000 plant safety approach has been specifically designed to maximize the plant robustness against catastrophic events resulting in extensive loss of infrastructure and a common-cause, complete loss of electrical power – both onsite and offsite. Specifically, the AP1000 plant is unique in that the plant response to a complete station blackout (SBO) is considered as a design basis event for mitigation of abnormal conditions and is embedded in the licensing basis.

It is this fundamental approach that is at the basis of the AP1000 robustness against extreme external events (Fukushima-like): the passive AP1000 plant was designed to eliminate unnecessary dependencies, thereby inherently creating a design safer and more independent for support function. This is portrayed in this statement by former U.S. NRC Commissioner William D. Magwood IV:

*“[…] had the plant been operating AP1000 [plant] reactors, it is likely that the outcome would have been very different. The AP1000 [plant]’s passive safety systems provide the ability to maintain core cooling for at least 72 hours with little human intervention. 72 hours to make repairs, transport emergency equipment, and other actions in response to the earthquake and tsunami that assaulted the Fukushima site would have made a very significant difference.”*

In response to the Fukushima Daiichi accident, Westinghouse performed lessons learned assessments for the AP1000 plant design. The post-Fukushima assessment confirmed that the passive AP1000 plant design is extremely robust against extreme external events that may lead to a complete and extended loss of power and infrastructure damage that could limit both availability of power as well as site accessibility. The passive safety systems, including the PXS and the PCS, ensure a minimum coping time of 72 hours even for severe Beyond Design Basis (BDB) events. Extension of this time requires minimal offsite support and use of pre-installed equipment or connections, with capability of delivery even in case of major damage to road or rail access. Even for extreme external events, the AP1000 plant design achieves and maintains safe shutdown, protects public health and safety, and prevents loss of utility investment.

Reviewing lessons learned is a hallmark of the nuclear industry and inherent to the Westinghouse safety culture. Consequently, Westinghouse established an internal expert team to perform a comprehensive review of the AP1000 plant design in consideration of the events at the Fukushima Daiichi nuclear power plant. The expert team was comprised of technical leaders from multi-disciplined Westinghouse engineering organizations, including Subject Matter Experts in safety system design, design for external hazards, plant layout, plant operations, PRA, deterministic safety analyses, and design for severe accidents. In addition to the Westinghouse internal review, several initiatives were launched worldwide to assess the lessons learned from the Fukushima Daiichi accident. These include, but are not limited to:

• European Nuclear Safety Regulators Group (ENSREG) stress tests [“EU Stress Tests Specifications, Annex 1,” May 25, 2011].

• The United Kingdom Office for Nuclear Regulation (ONR) Final Report [“Japanese Earthquake and Tsunami: Implications for the UK Nuclear Industry, Final Report,” September 2011].

• The International Atomic Energy Agency (IAEA) Expert Mission Report [“International Fact Finding Expert Mission of the Fukushima Dai-ichi NPP Accident Following the Great East Japan Earthquake and Tsunami,” May 24 – June 2, 2011].

• The United States Nuclear Regulatory Commission (US NRC) Near-Term Task Force [“Enhancing Reactor Safety in the 21st Century, The Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident,” July 12,2011].

The intent of the review was to challenge the AP1000 plant design and further evaluate the performance of the design when subjected to extreme hazards, such as those experienced at the Fukushima Daiichi site. The review team challenged the plant design for combinations of scenarios involving extreme external hazards and loss of station power sources. Information from the initial reviews was used to generate summary assessments of the AP1000 plant design’s ability to cope with SBO events, spent fuel pool (SFP) cooling, and external hazards. Videos describing the AP1000 plant SBO response for core and spent fuel pool decay heat removal can be found at the following:

http://www.westinghousenuclear.com/New-Plants/AP1000-PWR/Safety

For the review of these extreme situations, sequential loss of the lines of defense was assumed using a deterministic approach, irrespective of the probability of this loss. This approach allows for the evaluation of the levels of defense available following different external hazards, both within and beyond the design basis. The review focused on the impact of such extreme events relative to maintaining the key plant safety functions of core cooling, containment integrity, and spent fuel pool cooling. The review focused on the following issues:

• Initiating events – Earthquake, flooding (not limited to a tsunami), combination of both, and other potential limiting external hazards.

• Consequences of loss of safety functions from initiating events considered in the standard plant design – Loss of electrical power (including SBO), loss of Ultimate Heat Sink (UHS), and combination of both.

• Severe accident management issues – Means to protect from, and manage loss of, core cooling functions and cooling functions in the spent fuel pool; means to protect containment integrity.

One of the major differences of the AP1000 plant design when compared to current operating Pressurized Water Reactors (PWRs) is the extreme robustness of the design to loss of water makeup capability. Heat removal occurs in the following ways:

• Within the Nuclear Island, heat is removed first from the reactor core by the PXS, which has sufficient water inventory, protected inside containment to operate for long periods of time; heat is then removed from the containment by the PCS.

• The spent fuel decay heat is removed by heating up and boiling off the SFP water with steam released to the atmosphere through a vented path.

• Safety systems (in-containment water inventory, spent fuel pool water inventory, PCS water inventory) have sufficient capacity to support the safety functions for at least 72 hours. These passive safety systems are very robust against extreme beyond design basis events. Even credible beyond design basis events will not result in a challenge to the passive systems to fulfil their functions during the first 72 hours. After 72 hours, makeup will need to be provided to the top of containment and the SFP. This can be done through a variety of methods depending on operational preference or site-specific conditions.

Analyses have been performed and show that in the highly unlikely case of an operator not being able to supply water to the top of the containment after three days of cooling, air cooling alone will be sufficient to provide a High-Confidence, Low Probability of Failure (HCLPF) of the containment after 72 hours. The equilibrium containment pressure, while above the American Society of Mechanical Engineers (ASME) Service Level C pressure limit, still corresponds to a low probability of failure.

The robust design and exceptional performance in response to extreme external events results from the following three fundamental safety advancements:

• The AP1000 plant design is fail-safe – For station blackouts, critical SSCs will automatically achieve a fail-safe configuration without the need for operator action or AC/DC power.

• The AP1000 plant is self-sustained – The AP1000 plant passive approach to safety reduces the importance of AC power and cooling supply.

• The AP1000 plant is self-contained – The SSCs critical to placing the reactor in a safe shutdown condition are protected within the steel containment vessel and further surrounded by a substantial “steel concrete” composite shield building.

The Safe Shutdown Earthquake (SSE) is the basis for the design of the seismic Category I and II SSCs for the AP1000 plant. The seismic level of the SSE is 0.3g peak ground acceleration. This bounds the requirement of the EUR Document of 0.25g ground acceleration with no period of horizontal movement. The AP1000 plants have a higher peak ground acceleration than some competing designs. This additional margin is useful for coping with beyond design basis seismic events.

Additionally, the AP1000 plant is evaluated for a seismic margin analysis which extends to 67% above the SSE design basis peak ground acceleration (PGA) of 0.3g. This larger seismic event is referred to in the U.S. as the Review Level Earthquake (RLE), which has a PGA level for the AP1000 plant of 0.5g. For the AP1000 plant, seismic margin analyses demonstrate that the critical SSCs have a HCLPF level for seismic events equal to or greater than the RLE level. Even for beyond design basis seismic events, at least up to the Review Level Earthquake of 0.5g, the AP1000 provides a high confidence in a low probability of failure for critical SSCs.

More information on AP1000 plant design’s ability to cope with station blackout (SBO) events, spent fuel pool (SFP) cooling, and external hazards is also provided in the following:

* NPP\_NPP\_000065, Rev. 0, “AP1000 Nuclear Power Plant Coping with Station Blackout” [11]
* NPP\_NPP\_000067, Rev. 0, “AP1000 Nuclear Power Plant Spent Fuel Pool Cooling” [12]
* NPP\_NPP\_000072, Rev. 0, “Westinghouse AP1000 Nuclear Power Plant Response to External Hazards” [13]

# REGULATION RISK ASSEMENT CATEGORIES

In agreement with the purpose of this task during FEED is the identification of potential design risks and priorities for assessment work to be performed in a future project phase.

The High-Level Risk Assessments of this regulation is found in Section 5 of this document, attending to the compliance statements in section 4 of this document. Assigning it to one of the following risk categories:

1. Low risk: Compliance with regulations, codes, and standards are expected to be demonstrated without requiring a design change or requiring new design analyses.
2. Medium risk: Compliance with , codes, and standards are expected to be demonstrated without requiring a design change but requiring new design analyses.
3. High risk: Compliance with regulations, codes, and standards are expected to require a design change and potentially new design analyses.

The category assigned to each regulation, code or standard will be justified, and any identified gaps will be discussed.

Even though the scope of this Task 2 does not include a compliance matrix assessment for each regulation, code, and standard nor a line-by-line compliance matrix will at this stage. Some parts clauses are checked line by line in section.

# 

# DETAILED ASSESSMENT OF REGULATION CLAUSES AND REQUIREMENTS

This section provides the detailed assessment of the standard AP1000 plant design against the analyzed parts of the Safety Regulation [1]. Compliance is assessed by the compliance assessment categories identified in Section 2.1 and a justification is provided to support the compliance assessment.

## REGULATION 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. |
| COM-B | Compliant with planned update for Bulgaria Units | Full compliance with design modification or analysis/licensing scope planned for Bulgaria AP1000 plant project |
| 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. |

## CHAPTER I - GENERAL PROVISIONS

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 1 | | |
| (1) The current regulation defines the basic criteria and rules of nuclear safety and radiation protection of nuclear power plants, as well as the administrative provisions and the technical requirements for ensuring safety during the stages of site selection, design, construction, commissioning, and operation. | NR | Not a requirement. |
| (2) The Regulation also settles the requirements for industrial and fire safety, emergency planning and emergency preparedness of a nuclear power plant (NPP), as long as they result from implementation of the defence-in-depth concept. | NR | Not a requirement. |
| (3) This Regulation covers the physical protection of an NPP only in terms of the interrelations between physical protection measures and safety measures. | NR | Not a requirement. |
| Article 2 | | |
| (1) A nuclear power plant shall be assumed to be safe provided the following provisions have been simultaneously implemented:  1. The radiation impact of an NPP in all operational states is maintained below the prescribed dose limits for internal and external exposure of the personnel and the public, and is kept as low as reasonably achievable,  2. Accidents without fuel melting do not cause radiation impact which requires the implementation of public protection measures,  3. Accidents with fuel melting, resulting in early or large radioactive releases into the environment, are practically eliminated, while the other severe accidents (that are not practically eliminated) have only a limited radiation impact. | COM/  COM-B | This requirement has been assessed in other existing assessments for Bulgaria Project.   1. DCD chapter 12 provides principles to ensure that radiation impact is kept as low as reasonably achievable. This has been assessed in reference [7] as COM-B since it is recognized that new analyses need to be performed. 2. DCD chapter 15 provides radiological assessment of accidents without fuel melting. This has been analyzed in reference [7] as COM-P since calculations for accident analyses will need to be developed for Bulgaria Project. 3. DCD chapter 19 provides assessment of events with fuel melting. Practical elimination of accidents with fuel melting, resulting in early or large radioactive releases are practically eliminated, as presented in the report “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5] |
| (2) During the design and operation of an NPP and the implementation of all relevant activities, measures shall be taken to:  1. control the radiation exposure of people and releases of radioactive substances into the environment,  2. limit the frequency of events the occurrence of which may result in loss of core control or control of the fission chain reaction,  3. mitigate the consequences of such events if they occur. | COM | 1. The AP1000 plant is designed with administrative programs and procedures to maximize the incorporation of good engineering practices and lessons learned to accomplish As Low As Reasonably Achievable (ALARA) objectives as described in DCD [3] Chapter 12. The ALARA philosophy is applied in the AP1000 plant design. The design is reviewed for ALARA considerations and updated and modified as experience from operating plants is applied. ALARA reviews include the plant design and integrated layout, considering shielding, ventilation, and monitoring instrument designs as they relate to traffic control, security, access control, and health physics.   Radiation Protection Design Features are described in DCD [3] subsection 12.1.3. This Section includes the figures of AP1000 Radiation Zones on Normal Operation, Shutdown, and in Post Accident Conditions.  An additional assessment of this features is performed in BGP-GW-GL-202 [7].   1. Inherent nuclear feedback characteristics, e.g., Negative Reactivity Feedbacks, the negative fuel temperature reactivity effects, and the nonpositive moderator temperature coefficient of reactivity, are applied in the design to compensate increase in reactivity (see DCD sections 3.1 and 4.3). 2. Nuclear safety design principles, such as high safety margins, high-quality design of SSCs, redundancy, diversity, and physical separation, are applied in the design to ensure nuclear safety.   The plant is provided with the means of making and holding the core subcritical under any anticipated conditions and with appropriate margin for contingencies. Combined use of the control rod and the chemical shim control system permits the necessary shutdown margin to be maintained during long-term xenon decay and plant cooldown. The single highest worth control rod assembly is assumed to be stuck in the fully withdrawn position for this determination. |
| Article 3 | | |
| (1) The use of the defence-in-depth concept is the main tool for prevention and mitigation of accident consequences, and it shall be ensured with a suitable combination of:  1. an effective management system demonstrating the clear commitment of the NPP management to ensure priority of safety and development of a high level of safety culture.  2. selection of a suitable site and combining a conservative design with appropriate engineering solutions to provide diversity, redundancy, and safety margins, mainly through the use of:  a) design, technology and materials of high quality and reliability,  b) systems and design parameters that control and limit the reactor installation operation,  c) appropriate combination of inherent and engineered safety features.  3. comprehensive operating instructions and accident management procedures. | COM/ OR/ COM-B | (1) COM Defense-in-depth concept is applied in the design as presented in the DCD.   1. (OWN) Leadership and management for safety is a requirement of the Owner/Licensee, with regard to Westinghouse, management system promote nuclear safety and safety culture. 2. (COM-B) Site Selection Permit and Approval are Requested by the Bulgarian Act on The Safe Use Of Nuclear Energy . [6] (Articles 15 and 33), Site Approval is Requested in the Bulgarian Regulation on the Procedure for Issuing Licenses and Permits for the Safe Use of Nuclear Energy [] (Article 37). In the case of Kozloduy Site for Unit 7 Site Approval Order is granted by BNRA order No. АА-04-30. The compatibility of the site and site conditions are studied in report KZG-GW-GL-100 [9] and related to seismic and geotechnics in report KZG-GE01-X7R-001 [10]. Full compatibility of the proposed units with the conditions on site will need to be demonstrated taking into consideration the recommendations on these reports.   a) COM. AP1000 Quality Assurance is described in Chapter 17 of the DCD. Westinghouse Quality Management System QMS describes the Quality Assurance (QA) Program commitments to:  – ISO:9001 (Global Standard)  – 10 CFR 50 Appendix B (U.S. regulatory nuclear QA Program requirements)  – 10 CFR 21 and 10 CFR 50.55(e) (U.S. regulatory defect reporting requirements)  – NQA-1-2008, 2009 addenda (ASME QA Requirements for Nuclear Facility Applications)  – International Standards and Customer requirements (accomplished by applying a project quality plan or a WCAP Program Manual)  – Maintaining a healthy Nuclear Safety Culture  Westinghouse has and will continue to maintain a quality assurance program meeting the requirements of 10 CFR 50 Appendix B for the AP1000 program that will be applicable to the design, procurement, fabrication, inspection, and/or testing activities.  Design Reliability Assurance Program is described in DCD Section 17.4  b) COM. See DCD Chapter 16 Technical Specifications  c) COM. See sections 2.1.1 to 2.1.6 of this assessment.  3) OR/COM. Westinghouse provides a complete set of operating procedures for its scope of supply. Unit Owner shall develop specific procedures based on Westinghouse procedures Detailed operating instructions and accident management procedures are prepared during construction phase. |
| (2) The defence-in-depth concept shall be applied at all stages of the NPP lifetime. Depending on the activities performed, independent levels of safety shall be identified where no single technical, human or organisational error or fault may result in significant harmful consequences, and the combination of such errors or faults shall have a very low probability. | COM  OR | Defense-in-depth concept is applied in the design as presented in the DCD. The AP1000 plant design provides unique strengths in its defense‐in‐depth approach, particularly due to the high level of diversity, redundancy, and separation between highly reliable active systems designed to support normal operation and minimize the demand on the passive systems for anticipated events, and the safety‐related passive systems.  The levels of defense for accident prevention and mitigation contribute to low estimates for core damage probabilities while minimizing the occurrences of pressurization, heat‐up, and containment flooding.  This is accomplished by control, limitation, and protection systems. In addition, individual plant features, including the selection of appropriate materials, quality assurance during design and construction, well‐trained operators, and an advanced control system and plant design, provide substantial margins for plant operation before approaching safety limits. The approach includes dedicated features for severe accident management.  During NPP operation, application of defense-in-depth is in the responsibility of the Owner. |
| Article 4 | | |
| (1) A nuclear power plant shall be designed, sited, constructed, commissioned, and operated in such a way as to meet the safety objectives in the following areas:  1. normal operation, abnormal operation, and accident prevention,  2. accidents without nuclear fuel melting,  3. accidents with nuclear fuel melting,  4. independence of all levels of protection,  5. interrelation between safety and physical protection,  6. radiation protection and radioactive waste management,  7. competent management of activities and effective safety management. | COM  OR | NPP is designed, constructed, and commissioned according to the safety objectives as presented in the DCD.  Operation of the NPP is in the responsibility of the Owner. |
| (2) The safety objectives of normal operation, abnormal operation, and accident prevention are the following:  1. decrease the frequency of deviations from normal operation by increasing the capability of the NPP to remain stable within the operational limits and conditions;  2. limit the possibility of deviations from normal operation to evolve into accidents by increasing the NPP capability to control abnormal operation. | COM | AP1000 design criteria, operating characteristics and safety considerations are summarized in DCD section 1.2.1. It is considered that this requirement is fulfilled with the design criteria in DCD section 1.2.1 and design solutions presented in DCD. |
| (3) The safety objectives for accidents without nuclear fuel melting are to prevent fuel damage through engineering and administrative provisions while demonstrating that:  1. the probability of fuel melting has been minimized to the extent practicable by considering all types of failures, external events and hazards and their realistic combinations;  2. such accidents will not cause any radiological impact outside of the NPP site or will not require iodine prophylaxis, sheltering or evacuation as protection measures for the public;  3. release of radioactive substances from all sources of ionizing radiation has been minimized to the extent practicable.  4. at the stages of site selection and design, measures have been taken to decrease the impact of external events, hazards or malicious acts. | COM /COM-B | COM, AP1000 design criteria, operating characteristics and safety considerations are summarized in DCD section 1.2.1.   1. COM, The probability of fuel melting is minimized to the extent possible by the design principles and technical solutions presented in the DCD. The probability of fuel melting is assessed in DCD section 19. 2. COM-B. Accidents without fuel melting do not lead to severe radiological consequences. Radiological analyses from initiating events without fuel melting are presented in DCD section 15. This is analyzed in BGP-GW-GL-202 [7]. 3. Releases are minimized to the extent possible by the design principles and technical solutions presented in the DCD, see e.g., See, for the standard design, DCD section 12 regarding ALARA principle, and DCD subsection 11.5.3 Effluent Monitoring and Sampling contains information on this respect. DCD subsection 11.2.3 Radioactive Releases discuss Liquid Releases for a Single Unit, summarized in Table 11.2-7, subsection 11.3.3 discusses radiation releases and doses at the site Boundary due to activity released as a result of normal operations. This is analyzed in BGP-GW-GL-202 [7] as COM-B 4. Site selection approval is granted in the case of Kozloduy Unit 7 under the specified condition in site approval order. Impact of external events, hazards and malicious acts are considered in the design of AP1000 as presented in the DCD, see e.g., DCD Chapter 2, DCD section 3.4 regarding external flooding, section 3.5 regarding external missiles and section 3.7 regarding seismic events. See Article 3 in this report where this is assessed as COM-B. |
| (4) The safety objectives for accidents with nuclear fuel melting are intended to decrease possible radioactive releases to the environment both during the accident (in the reactor and in the spent nuclear fuel pool), and for a longer period (defined by considering the time needed to maintain safety functions) while meeting the following criteria:  1. accidents with nuclear fuel melting, resulting in early or significant radioactive releases to the environment shall be practically eliminated;  2. for accidents with nuclear fuel melting that cannot be practically eliminated, design modifications shall be implemented such that only public protective actions that are limited in terms of lengths of time and areas of application would be necessary (without permanent resettlement or evacuation except for the areas in the vicinity of the NPP, limited sheltering, and without long-term restrictions for consumption of foodstuffs), and sufficient time shall be available to implement these measures. | COM  OR | AP1000 design includes several design solutions to decrease possible radioactive releases to the environment as presented in the DCD.   1. Practical elimination of accidents with fuel melting, resulting in early or large radioactive releases are practically eliminated, as presented in the report “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5] 2. AP1000 includes design solutions to ensure that public protection actions are limited. Design solutions against accidents with fuel melting are presented and analyzed comprehensively in DCD section 19. This analysis supports the technical basis for simplification of offsite emergency planning. The offsite emergency planning is discussed in DCD section 13.3.   Emergency response activities are responsibility of the Owner. |
| (5) In order to reach an overall strengthening of the defence-in-depth to the extent practicable, the independence of all protection levels shall be increased, particularly by using the diversification principle. | COM | Independence of defense-in-depth is increased by applying safety principles in the design, including e.g., diversity, functional isolation, and physical separation, presented in several sections of the DCD. |
| (6) The safety objective under para. 1, item 5 is to design and apply the safety measures and physical protection measures in a well-considered and harmonious manner. Safety and physical protection shall be enhanced concurrently. | COM | Safety and physical protection are considered in the AP1000 design. Safety design features are presented in DCD and physical protection features in separate AP1000 Security Design Report. |
| (7) The safety objectives under para. 1, item 6 are that under all operating states through design modifications the following shall be minimized to the extent practicable:  1. individual dose and collective dose to the personnel;  2. radioactive releases to the environment;  3. radioactive waste quantities and activity levels. | COM | ALARA-principle is applied in the AP1000 design to minimize the effects of radiation under all operating states as presented in DCD section 12. |
| (8) The safety objective under para. 1, item 7 is to achieve competent management of the activities and effective safety management, starting at the design stage. This requires the operating organisation to:  1. establish effective safety management of the NPP design, and have competent personnel and sufficient available technical and financial resources to bear full responsibility for ensuring safety.  2. implement such measures that allow the staff of all other organisations involved in site surveys, design, construction, commissioning and operation to demonstrate their awareness of safety issues related to their job or their personal role in ensuring safety. | OR  COM | Requirement is mainly related to Owner.  DCD section 17 outlines quality assurance program applicable to the design, procurement, fabrication, inspection, and/or testing of items and services for the AP1000. |

## CHAPTER 3 - SITE CHARACTERISTICS

### Section I: General Requirements

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 28 | | |
| The characteristics of potential NPP sites and of the selected site shall be assessed and documented as an integral part of the overall NPP safety analysis. | OR / COM-B | Identification of Site-specific Potential Hazards as an action required by The Owner.  DCD Chapter 2 identifies bounding site characteristics and hazards for which the AP1000 plant has been designed. Site-specific reconciliation is performed on a project-specific basis. The compatibility of the site and site conditions are studied in report KZG-GW-GL-100 [9] and related to seismic and geotechnics in report KZG-GE01-X7R-001 [10]. Full compatibility of the proposed units with the conditions on site will need to be demonstrated taking into consideration the recommendations on these reports.  AP1000 design is protected against internal and external hazards as presented in several sections of the DCD (e.g., DCD section 3) and confirmed with probabilistic safety analyses (see DCD section 19). However, further considerations may be needed to document site-specific characteristics . |
| Article 29 | | |
| (1) The following groups of characteristics shall be identified during the NPP site selection:  1. External impacts of natural origin that may affect the NPP;  2. External impacts of human induced origin that may affect the NPP;  3. Site characteristics that affect the NPP impact on the public and environment (dispersion of radioactive substances, population density). | N/A | Site is already approved [19]. |
| (2) The site selection shall be based on a comprehensive weighted analysis of all characteristics and priority given to those that have a direct impact on the NPP safety and security. | N/A | Site is already approved [19]. |
| Article 30 | | |
| (1) The assessment of processes, phenomena, and factors of natural and human induced origin for the selected site shall confirm the possibility for taking protective measures to prevent their impact and meet the safety objectives under Article 4. | NAS | Site is already approved [19].  AP1000 Design includes technical solutions to manage external events.  The AP1000 plant design approach is to have a standardized design which bounds an established set of site characteristics and external hazards that are expected to be common to multiple sites. In addition, site-specific external hazards will be reviewed to confirm the bounding analyses are not impacted by site specific characteristics. DCD Chapter 2 identifies the site characteristics. DCD Chapter 3 describes the design of structures, systems, and components (SSCs) with respect to external hazards such as wind and tornado loadings, flooding, missiles, and seismic design. External events are also addressed in the PRA as described in DCD Section 19.58.  The design of the AP1000 plant nuclear safety systems and engineered safety features includes allowances for natural environmental disturbances such as earthquakes, floods, and storms at the station site. The nuclear island structures are designed to withstand the effects of natural phenomena such as hurricanes, floods, tornadoes, tsunamis, and earthquakes without the loss of capability to perform safety functions. Design for natural phenomena is based on the industry standards as described in DCD Chapters 2 and 3. Those systems, structures, and components vital to the shutdown capability of the reactor are designed to withstand the envelope of probable natural phenomena described in DCD Chapter 2. Specific sites are evaluated with respect to the standard AP1000 plant site envelope to assure site specific safety capabilities.  SSCs important to plant protection are designed to maintain their functionality and integrity when subjected to potential probable hazards that could challenge plant safety as described in DCD Chapter 3.  However, requirement fulfilment can be completely confirmed when site specific safety analyses are completed. This will need to be studied taking into account the recommendations and discussions on references [9], [10]. |
| (2) When the site under consideration for a new NPP is in close proximity to the site of an existing NPP, account shall be taken of the impact of the existing nuclear facilities. | OR/COM-B | Selected site includes existing nuclear facilities. This may need further considerations in the design and safety analyses. |
| Article 31 | | |
| Siting of NPP is not allowed:  1. in territories where this is forbidden by a normative act, or on sites that do not meet the requirements for environmental protection, radiation, fire safety and physical protection, or any other requirements stipulated by a normative act;  2. on sites where practical measures cannot be implemented to prevent large or early releases of radioactive substances into the environment as a result of external impacts;  3. on sites of pronounced seismic activity combined with surface deformations;  4. on sites located up to 5 km away from a known capable fault or its branching where a break and/or deformation on or near the ground surface may be expected;  5. on sites with a potential danger of old or new landslides being activated;  6. on sites of nonconsolidated soils or with a potential for liquefaction, subsiding, sinking, pitching terrain, or erosion of slopes where the implementation of safety ensuring engineering measures is practically impossible;  7. on sites where karst, sufosis and karst-sufosis processes take place;  8. on sites within the zones of passage of snow avalanches or mud streams, and in areas of mud volcano activity;  6. on sites exposed to impact of tsunami waves;  10. on mine development sites the stability of which cannot be ensured;  11. on sites of active exchange of surface and ground waters. | N/A | Site is already approved by Bulgarian Nuclear Regulatory Agency Order No. АА-04-30. 21.02.2020. By which BNRA Approves: "the site selected by KOZLODUY NPP – NEW BUILDS PLC (UIC 202058513) for the siting of a nuclear facility - nuclear power plant (Site No. 2) with a location, boundaries and characteristics according to the submitted documents"[19]. |

### Section II: Studies of Natural and Human Induced Factors for Site Selection

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 32 | | |
| The following engineering surveys and studies of processes, phenomena and factors of natural origin that may impact the NPP safety shall be conducted for the NPP location region and the NPP site:  1. The following tectonic activity characteristics shall be defined:  а) location of faults, potential earthquake foci zones and geodynamic zones with respect to the NPP site, indicating the orientation and boundaries of potentially hazardous fault zones;  b) amplitudes, speed and gradients of the latest and contemporary movements of the earth crust, parameters of potential dislocations;  c) characteristics of the capable fault areas (geometric schemes, dislocation amplitudes and directions along the faults, data of the latest activity known);  2. The following shall be identified within the site boundaries:  a) characteristics of seismic movement (accelerations, speed, dislocations, response spectra) of an earthquake with frequency of events of at least 10-2 events per year (seismic level - 1), and for a safe shutdown earthquake (SSE) with frequency of at least 10-4 events per year (seismic level -2) at the level of the natural terrain of the site;  b) hazard of landslide displacements of the slopes considering the ground layer conditions and seismic fluctuations with an intensity of up to safe shutdown earthquake including, and also when the impact of ground waters, tectonic deformations and contemporary geodynamic processes are considered;  c) possibility of karst, sufosis and karst-sufosis processes development;  d) presence of specific ground layers (biogenic, sinking, swelling, saline, alluvial, human induced), the thickness of these layers and their physico-mechanical properties (deformation moduli, strength properties, etc.);  e) areas of water-saturated unconnected layers susceptible to liquefaction during seismic impacts, and the boundary values of ground acceleration with potential for liquefaction;  f) uplift of groundwater level and flooding of the site as a result of spreading of ground water uplift coming from dams, filtration from irrigated lands, water flows, precipitation, snow melting;  g) rare phenomena characteristics such as windspouts (tornadoes) (including their frequency of occurrance, intensity, maximum tangential values at the periphery and tornado forward movement speed, drop of pressure between the periphery and the centre of the tornado);  3. The following shall be defined for an NPP site: the maximum water level and the duration of possible flooding due to precipitation, intensive snow melting, high water level in water bodies, ice blocking of rivers, avalanches and slides; the characteristics of probable maximum run off floods from watercourses with a frequency of 10-4 events per year combined with high tides and waves caused by winds shall be also evaluated;  4. The probability of occurrence and the maximum height of tsunami or seiches waves, considering the seismic tectonic conditions, shore configuration, landslides and collapse in the water, shall be evaluated for an NPP site situated at the coast of a sea, lake or dam;  5. The impact on safety of other processes, phenomena and factors of natural origin (hurricane, extreme precipitation, icings, thunderstorms, dust-storms and sand-storms, erosion of river and water body banks) shall be determined for an NPP site. | NAS | Site is already approved [19].  The AP1000 design is protected against internal and external hazards. However, further considerations may be needed to confirm that these site-specific external events are covered by the AP1000 design. |
| Article 33 | | |
| (1) The region of an NPP location and its respective site shall be investigated to identify sources of potential human induced hazards irrespective of their frequency (recurrence). | NAS | Site is already approved [19]. Further considerations may be needed to confirm that site-specific human induced hazards are covered by the AP1000 design. This will need to be studied considering the recommendations and discussions on references [9], [10]. |
| (2) Sources shall be identified of human induced hazards that may cause explosions, fires, releases of explosive, toxic, and corrosion-active substances. | OR | Site is already approved [19]. Further considerations may be needed to confirm that site-specific human induced hazards are covered by the AP1000 design. This will need to be studied considering the recommendations and discussions on references [9], [10]. |
| (3) All potential stationary and mobile sources of explosions, including industrial and military sites for production, processing, storage and transportation of chemicals and explosive substances, and ammunition dumps shall be analysed and the impact parameters shall be identified for the most dangerous explosion. | OR | Site is already approved [19].  The AP1000 Standard Design satisfies the required separation distances between potentially explosive chemicals and SSCs. The design has been developed in accordance with U.S. NRC Regulatory Guide 1.91, which defines the safe distance from an explosion (see DCD Table 2.2-1) as the point at which the blast wave overpressure is limited to approximately 7 kPa (1 psi); below this level no significant damage would be expected. This criterion has been used for On-Site Explosions, Offsite Explosion are site Specific and will need to be checked, such as the Table IX 2-30 of the Kozloduy PSAR, see reference [9].  Nonetheless it has to be noted that as a result of the nuclear island’s design to withstand such extreme events as the SSE, the nuclear island structures are inherently designed to resist an off-site explosion. As was stated in IAEA Safety Guide NS-G-1.5 notes, structures will often have been designed to accommodate extreme loadings such as those resulting from aircraft impacts, tornado-generated pressure and missile loads or earthquakes. This IAEA guide stated that structures with reinforced concrete walls that are a minimum of about 0,5 m thick and seismically designed should be capable of withstanding overpressures generated by external explosions.  The AP1000 plant nuclear island external walls are all seismically designed and thicker than 0,5 m. For example, the shield building has a nominal wall thickness of 0,914 m. Based on the IAEA guidance, such structures should be capable of withstanding substantial overpressures house.  It is unnecessary, therefore, to apply additional design measures to mitigate the effects of design basis external explosions, unless their effects are found to be more severe than those corresponding to the other extreme loadings already considered, if such a case is possible additional design measure might need to be studies |
| (4) All stationary and mobile potential sources of emergency release of chemically active substances, including industrial and military sites for processing, use, storage and transportation of toxic and corrosive substances shall be analysed. | OR | Site is already approved [19]. Further considerations may be needed to confirm that site-specific hazards related to chemical substances are covered by the AP1000 design. |
| (5) The impact parameters on an NPP and the respective probabilities shall be determined for events induced by:  1. explosions and fires, releases of explosive, inflammable, toxic and corrosive gases and substances from industrial facilities, ground and water conveyance facilities;  2. a modern passenger aircraft crash;  3. floods, including those related to reaching the waterfront as a result of breaking of dams located upstream of the NPP site;  4. accidents of a water vessel along water routes and in harbour zones occurring together with explosions and fires, releases of dangerous chemicals, provided the NPP is situated within their range of impact;  5. electromagnetic emissions (fields);  6. external fires (forest areas, peateries, flammable liquids);  7. deformations and other factors arising on developing underground resource deposits, carrying out excavation works, including tunnel construction, mines and quarries exploitation and their emergency destruction;  8. water level fluctuations of the NPP water supply source. | OR/COM-B | Site is already approved [19]. Further considerations may be needed to confirm that site-specific hazards are covered by the AP1000 design. This will need to be studied considering the recommendations and discussions on references [9], [10].  2. Regarding aircraft crash, detailed assessment is performed in DCD section 19, appendix F.  Deterministic aircraft crash (ACC) analyses for intentional aircraft have been performed for the AP1000 plant design. Detailed ACC analyses have been performed that demonstrate that the AP1000 plant is robust enough to ensure confinement of radioactive releases and maintain adequate core cooling.  Westinghouse has performed a rigorous assessment of the AP1000 plant design to demonstrate that the plant’s design features and functional capabilities provide inherent protection against the effects of an aircraft impact. Westinghouse aircraft impact assessments have been subjected to the detailed reviews in both the US and Europe from an independent peer panel, the NRC and the UK Office of Nuclear Regulation (ONR). All three reviews accepted the conclusion that an aircraft impact would not inhibit the plant’s core cooling capability, would not impact containment integrity and would not impact spent fuel pool integrity based on best-estimate assessments.  The AP1000 plant assessments for aircraft impact meet the requirements of Nuclear Energy Institute’s NEI 07-13, “Methodology for Performing Aircraft Impact Assessments for New Plant Designs,” and US Nuclear Regulatory Commission (NRC) Regulatory Guide 1.217, “Guidance for the Assessment of Beyond-Design-Basis Aircraft Impacts.” NEI 07-13 requires the following effects to be examined as part of the evaluation:  - Structural analysis: an assessment of the effects of aircraft fuselage and wing structure is performed.  - Shock and vibration: an assessment of the effect of shock-induced vibration on systems, structure, and components is performed.  - Localized structural analysis: an assessment of the penetration of hardened aircraft components, such as engine rotors and landing gear is performed.  - Fire effects and secondary impacts: if perforation of analyzed structural components is predicted, realistic assessments are conducted of the damage to internal SSCs caused by burning aviation fuel and secondary impacts.  The assessment criteria require that the following be demonstrated using realistic analysis:  - The reactor remains cooled, or the containment integrity remains intact.  - Spent fuel cooling is maintained.  The Shield Building is a key design feature for the protection of the safety systems located inside containment from the impact of a large commercial aircraft. The assessment concluded that a strike upon the shield building would not result in perforation of the Shield Building’s inner steel liner; therefore, damage to the containment vessel would not occur.  Therefore, the systems and equipment within the containment vessel would not be damaged from the impact or from the exposure to jet fuel. The safety-related components inside containment, including the reactor pressure vessel and Passive Core Cooling System, remain intact and maintain their intended capabilities following the shock-induced vibrations resulting from the impact of a large commercial aircraft.  The aircraft impact assessment conclusively demonstrates the capability of the AP1000 plant to continue to provide adequate protection of public health and safety by showing that core cooling capability, containment integrity, Spent Fuel Pool integrity and adequate spent fuel pool cooling are maintained. An intentional aircraft impact does not lead to core melt. |
| Article 34 | | |
| (1) The factors that affect the NPP impact on the public and the environment shall be considered during the NPP site selection. | N/A | Site is already approved [19]. |
| (2) The aerologic, hydrometeorological, hydrogeological and geochemical conditions of radionuclide dispersion, migration and accumulation, and also the natural radiation background shall be studied in the monitored area and predictions shall be made for changes in these conditions over the NPP operating lifetime. | OR | Site is already approved [19]. Further considerations may be needed to confirm that site-specific conditions are covered by the AP1000 design. |
| (3) Atmospheric dispersion shall be assessed by taking into consideration slight wind, calm weather, air temperature, near-surface and altitude inversions, atmospheric stability, precipitation and fogs in the region of the NPP site. | OR | Site is already approved [19]. Further considerations may be needed to confirm that site-specific conditions are covered by the AP1000 design. |
| (4) The characteristics of radionuclide migration in surface- and ground-water and deposition of radionuclides at the bottom of water bodies shall be defined considering the following:  1. possible radioactive contamination of drainage and groundwater;  2. radionuclides physical and chemical properties;  3. kinetics of geochemical reactions and possible changes in the mineralogical makeup of layers;  4. lithological composition and thickness of water-bearing and watertight strata, the earth layers in the weathering zone and the soil layer;  5. sorption capacity of sediments, earth layers and soil layers with respect to radionuclides and hazardous chemical substances;  6. direction and speed of contaminated streams towards the release places (drain-pipes, water bodies, water intake wells, etc.); | OR | Site is already approved [19]. Further considerations may be needed to confirm that site-specific characteristics are covered by the AP1000 design. |
| Article 35 | | |
| To ensure reliable and long-term residual heat removal of nuclear fuel, the extreme temperatures of water and air and their duration, air humidity, water flow rate, minimum water level, and quantity of algae shall be specified. | OR | Site is already approved [19]. Further considerations may be needed to confirm that site-specific conditions are covered by the AP1000 design. This will need to be studied considering the recommendations and discussions on references [9], [10].  Unique to the AP1000 plant design is the use of the steel containment vessel with cooling from the Passive Containment Cooling System (PCS). This provides a path for the removal of decay heat from the containment atmosphere to the environment as the safety-related ultimate heat sink. The AP1000 plant has been designed so that an extreme ambient temperature within the design basis will not prevent the delivery of key safety functions, however some analyses have been performed for higher temperatures than those stated as the maximum design safety temperatures. The maximum and minimum external design temperatures are 46,1°C (115°F) and -40°C (-40°F) respectively, AP1000 taking into account the passive safety features of the design, will not suffer a complete loss of its safety functions but a progressive deterioration of these passive safety systems performance (e.g. less heat been rejected to a hotter environment as Ultimate Heat Sink, or more probability of failure of some components), thus no cliff edge effects are determined. |
| Article 36 | | |
| (1) The current and future distribution of population and use of land and water sources within the region of the NPP shall be identified for the purposes of emergency planning. | OR | Emergency planning is in the responsibility of the Owner. |
| (2) To determine the population distribution, data from the latest population census, revised in terms of the direction and distance to the NPP, shall be used. | OR | Emergency planning is in the responsibility of the Owner. |
| (3) The study on land and water sources use by the population provides the data that are used in the food chain for identifying the NPP radiological impact on the population. | OR | NPP radiological impact assessment on the population is the responsibility of the Owner. |
| Article 37 | | |
| (1) Studies, analyses and engineering works shall be performed efficiently and in good quality at all stages of the NPP site investigation. | OR/COM | Site is already approved [19]. Further studies are needed considering the recommendations and discussions on references [9], [10]. |
| (2) Engineering investigations shall be carried out in sufficiently large regions and areas to cover all special features and spheres of influence that may be of importance for identification of natural and human induced hazard sources, and the characteristics of the studied events. | N/A | Site is already approved [19]. |
| (3) To describe natural and human induced hazards, suitable design parameters shall be chosen or developed while considering the uncertainties of data used for investigations and studies. | OR | Requirement for the Owner. |
| (4) An NPP site meteorological monitoring programme shall be developed and implemented to measure the basic meteorological parameters at appropriate heights and places. Data from at least a year back shall be processed together with all related data from other sources. | OR | Requirement for the Owner. |
| (5) Results of field researches, laboratory tests, geotechnical analyses and other studies shall be incorporated in a sufficiently detailed report allowing for independent assessment. | OR | Requirement for the Owner. |

## CHAPTER 4 - DEFENCE IN DEPTH AND DESIGN BASIS

### Section I: Defence in Depth Implementation in the Design

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 38 | | |
| The defence in depth concept shall be implemented in the design through provision of a number of physical barriers and several levels of protection for ensuring protection against the impact of ionizing radiation and consequences mitigation in case of preventive measures failure. | COM | Structural and functional defense-in-depth concept is applied in the AP1000 design as presented in the DCD.  The DCD as a whole demonstrates that the concept of defense in depth is applied in the AP1000 plant design. US NRC design criteria that are equivalent to the criteria in paras. 2.21 to 2.18 of SSR-2/1 are explained in DCD Section 3.1. Westinghouse provided compliance assessment against the SSR-2/1 document: APP-GW-GL-059 [24] with additional information.  DCD Chapter 6, 9, 15, and 19 provide additional supporting information.  EPS-GW-GL-701 [25] discusses in more details the AP1000 plant compliance with the concept of defense in depth.  The AP1000 plant design provides for multiple levels of defense for accident mitigation (defense-in-depth), resulting in extremely low core damage probabilities while minimizing the occurrences of containment flooding, pressurization, and heat-up. Defense-in- depth is integral to the AP1000 plant design, with a multitude of individual plant features capable of providing some degree of defense of plant safety. The AP1000 plant provides defense-in- depth protective barriers as described in the AP1000 plant DCD Section 3.1.2.  The AP1000 plant design for stable, normal operation prevents challenges to the integrity of the physical barriers. In addition, the materials used to provide physical barriers have been shown to have a low probability of failure. Refer also to the discussion of the AP1000 plant compliance with US NRC GDCs 14. 16, 30, 31 in DCD Chapter 3.  The accident analyses presented in DCD Chapter 15 demonstrate how failure of a barrier is prevented when challenged, by the failure of another barrier or another event. Refer also to the discussion of the AP1000 plant compliance with US NRC General Design Criteria (GDC) 14, 16, 30, 31 in DCD Chapter 3. An additional level of defense for failure of a barrier as consequence of another barrier is provided through the diverse mitigation functions within the passive safety systems.  Containment integrity is further protected by the next level of defense-in-depth, i.e. the availability of certain systems for reducing the potential for events leading to core damage. Severe accident mitigation guidelines (SAMGs) provide guidance to the operators and emergency response personnel on how to respond to a plant emergency where specific plant parameters have reached a point where core damage may have occurred. The AP1000 plant design provides the operators with the ability to drain the in-containment refueling water storage tank water into the reactor cavity in the event that the core has uncovered and is melting. This prevents reactor vessel failure and subsequent relocation of molten core debris into the containment. Retention of the debris in the vessel provides for a high confidence that containment failure and radioactive release to the environment will not occur due to ex-vessel severe accident phenomena. Analysis also shows there is a high confidence of a low probability of failure of the containment vessel if passive containment water cooling is maintained for 3 days and only air cooling is assumed afterwards. |
| Article 39 | | |
| (1) The number of the necessary physical barriers shall be specified on the basis of an assessment of quantities and isotope composition of radionuclides that might be released into the environment, the efficiency of the different barriers, their vulnerability to internal and external impacts, as well as the potential consequences in case of a failed barrier. | COM | Physical barriers and their efficiency are specified and analysed in the DCD. Comprehensive structural (DCD section 3), deterministic and probabilistic safety analyses (DCD sections 15 and 19) are performed to verify the efficiency of the barriers during normal operation and in case of initiating events and hazards. |
| (2) The NPP design shall envisage independent physical barriers for each significant source of ionizing radiation. The assessment under para. 1 shall cover both all risks caused by all the nuclear fuel on the NPP site, and the risks due to other sources of ionizing radiation. | COM | Independent physical barriers are designed for prevention of radioactive releases. Comprehensive structural (DCD section 3), deterministic and probabilistic safety analyses (DCD sections 15 and 19) are performed to verify that there are sufficient design solutions to manage risks from ionizing radiation. |
| Article 40 | | |
| (1) The levels of defence shall have the objective of preventing the following to the extent practicable:  1. conditions leading to breaking the integrity of the physical barriers;  2. failure of a physical barrier when challenged (under the conditions of item 1.);  3. failure of a physical barrier as a consequence of a failure of another physical barrier;  4. possibility of unfavourable consequences resulting from errors in the operation and servicing of structures, systems and components (SSCs). | COM | Independence and integrity of physical barriers are considered in the AP1000 design. Comprehensive structural (DCD section 3), deterministic and probabilistic safety analyses (DCD sections 15 and 19) are performed to verify that there are sufficient design solutions for events jeopardizing the physical barriers. |
| (2) The purpose of the first level of defence shall be to prevent abnormal operation, failures of SSCs important to safety which necessitate a conservative layout, design, construction, maintenance and operation of the NPP in compliance with a management system and proven engineering practices. This objective shall be accomplished with the help of:  1. selection of appropriate design standards and materials;  2. quality control during component manufacturing, construction and commissioning;  3. decreasing the risk of internal hazards;  4. application of processes and procedures for NPP design, manufacturing of components, construction of the NPP, maintenance, surveillance and testing of important to safety SSCs;  5. the method of operation and consideration of operating experience;  6. detailed analyses of the operation, maintenance and management system. | COM  OR | Defense-in-depth concept is applied in the AP1000 design. Items 1-6 in the Article are part of the AP1000 design features presented in the DCD.  Operation, maintenance and testing related topics in this Article are also requirements for the Owner. |
| (3) The purpose of the second level of defence shall be to detect and control deviations from normal operation to prevent anticipated operating occurrences escalating into accident conditions. The second level of defence shall require:  1. the design to provide systems and design features that control and limit the reactor facility operation;  2. efficiency of design systems and features to be verified by safety analyses;  3. development of operating procedures to prevent deviations from normal operation and anticipated operational occurrences, to mitigate their consequences and return the NPP to a safe state. | COM | Defense-in-depth concept is applied in the AP1000 design. Items 1-3 in the requirement are part of the AP1000 design features presented in the DCD.  Development of operating procedures will be done during construction phase. |
| (4) The objective of the third level of defence shall be to prevent nuclear fuel damage and off-site release of radioactive substances; to bring the reactor installation to a safe state in case of anticipated operational occurrences and accident sequences, through the use of the inherent safety features, and safety systems and emergency procedures envisaged for that purpose. | COM | Defense-in-depth concept is applied in the AP1000 design. Requirement is considered in AP1000 design features presented in the DCD.  Generic AP1000 Emergency Operating Procedures (EOPs) mitigate the consequences of an accident and periodically reviewed. There is a training program developed within the accident management guidelines to provide preparedness to the personnel who would be involved in accident mitigation actions. |
| (5) The purpose of the fourth level of defence shall be to control and manage accidents that have occurred at precedent levels of defence or were caused by extreme external events in order to return the reactor installation to a stable safe state and postpone in time the consequences of severe accidents. At this level, the most important task is to ensure the function for retaining radioactive substances within the containment, thus decreasing radioactive releases into the environment to a level as low as reasonably achievable. | COM | Defense-in-depth concept is applied in the AP1000 design. Requirement is considered in AP1000 design features presented in the DCD.  Generic AP1000 Severe Accident Management Guidelines (SAMG) are developed to mitigate the consequences of an accident and periodically reviewed to accommodate changes that may affect the mitigation strategies. There is a training program developed within the accident management guidelines to provide preparedness to the personnel who would be involved in accident mitigation actions. |
| (6) The purpose of the fifth and last level of defence shall be to mitigate the radiological consequences to the public caused by radioactive releases as a result of possible accident conditions. This requires that an adequately equipped emergency response centre, emergency plan and emergency procedures, and an off-site emergency response should be in place. | COM  OR | Defense-in-depth concept is applied in the AP1000 design. Requirement is considered in AP1000 design features presented in the DCD.  Operative emergency planning and procedures are part of the Owner’s requirements. |
| Article 41 | | |
| (1) The implementation of the defence in depth shall ensure that each level of defence be independent and efficient at all times so that the loss or inefficiency of one of the defence levels shall not affect the functionality of the other levels. | COM | Defense-in-depth concept is applied in the AP1000 design. Independency of the defense-in-depth levels is comprehensively analyzed in deterministic and probabilistic safety analyses (DCD sections 15 and 19). |
| (2) Independence of SSCs performing safety functions at different levels of defence shall be ensured by simultaneously meeting the following conditions:  1. the capability to perform the required safety functions shall not be influenced by the operability or inoperability of SSCs which are part of safety functions at other levels of defence;  2. the capability to perform the necessary safety functions shall not be influenced by the consequences of postulated initiating events, internal and external hazards including, which require the functioning of the respective SSC. | COM | Defense-in-depth concept is applied in the AP1000 design. Independency of the defense-in-depth levels is comprehensively analyzed in deterministic and probabilistic safety analyses (DCD sections 15 and 19). |
| (3) The design shall ensure adequate efficiency of the first two levels of defence to prevent the escalation into accidents of all failures or abnormal operation that may occur throughout the whole operational lifetime of the NPP. | COM | Defense-in-depth concept is applied in the AP1000 design. Independency of the defense-in-depth levels is comprehensively analyzed in deterministic and probabilistic safety analyses (DCD sections 15 and 19). |
| (4) Systems and means for prevention of accidents with nuclear fuel melting shall be independent of systems and means specially designed to perform safety functions in case of a postulated severe accident to such an extent as not to impede the implementation of these functions. | CWO | There are SSCs which are used both during transients and during accidents with fuel melting, such as Passive Containment Cooling System. However, operation of these systems during transients do not affect to the operation during accidents with fuel melting.  Due to the passive features with high reliability in AP1000 design, it is considered that objective of this requirement is achieved. This is confirmed by deterministic and probabilistic safety analyses (DCD sections 15 and 19). |

### Section II: Design Basis

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 42 | | |
| The design basis shall specify the characteristics of NPP and its SSCs necessary to perform safety functions for the purpose of:  1. ensuring safe operation within justified operational limits and conditions throughout the entire operational lifetime;  2. mitigation of potential radiological impact within the boundaries of the NPP site so that in all operational states and accidents without fuel melt to avoid reaching the intervention criteria and taking protection measures for the public as stipulated in the Regulation pursuant to Article 123 of the Safe Use of Nuclear Energy Act;  3. prevention of accident progression and melting of nuclear fuel in the reactor core and the spent fuel pool;  4. prevention of practically eliminated large or early releases of radioactive substances into the environment;  5. mitigation of consequences from potential releases from accidents that could not be practically eliminated, long-term localization of radioactive substances and maximum delay in time of eventual leakage. | COM | According to Bulgarian Regulation [1] “Design basis” shall mean the range of conditions and events taken explicitly into account in the design and the improvements of a nuclear power plant, according to established criteria, so as not to exceed authorized limits through the intended activity of SSCs that perform safety functions. This definition is aligned with that of the Council Directive 2014/87/EURATOM [20]  The design basis of AP1000 and its SSCs are presented in the DCD and verified in deterministic and probabilistic safety analyses (DCD sections 15 and 19).  Operating limits and conditions are specified in DCD section 16, and will be updated, if necessary, during construction and commissioning phase of the NPP.  The fulfilment of the Act on Safety Use of Nuclear Energy is assessed in separate requirement assessment [6].  Practical elimination is evaluated in separate report “AP1000 Plant methodology for Demonstration of Practical Elimination” [5]. |
| Article 43 | | |
| In all operating states of the nuclear facilities on the NPP site, the annual individual effective dose resulting from internal and external exposure of the public caused by the impact of all nuclear facilities on-site shall be maintained as low as possible and shall not exceed 0,15 mSv. | COM-B | The ALARA principle is applied in the design as presented in DCD section 12. The annual dose limit requirement may need further evaluations for AP1000 design.  A specific calculation will be needed for doses and releases in normal Operation, this was discussed explained in Feasibility Study [21] subsection II-2.1.2 Evaluation of the Capacity of the Site, the expectation with current data and the analogy with the releases of the current operating facilities on site is that dose constraints can be met. Some recommendations were developed in that study.  Therefore, due to the design solutions for preventing radioactive releases, it is currently expected that this article will not lead to design changes. This is also assessed in [7]. |
| Article 44 | | |
| (1) The NPP design shall have the necessary characteristics allowing for minimizing to the extent practicable the probability of nuclear fuel melting by considering all failures, external and internal hazards and realistic combinations of events. | COM | AP1000 design has the necessary characteristics to minimize the risk of nuclear fuel melting to the extent possible in different events as presented in the DCD. This is confirmed by deterministic and probabilistic safety analyses (DCD sections 15 and 19) and Design PRA [4]. |
| (2) The safety assessment under para. 1 shall confirm that the mean value of the nuclear fuel melting frequency is less than 10-5 a year for a nuclear power unit based on the consideration of all operating states and all types of initiating events and hazards. | COM-B | DCD section 19.59 presents results of probabilistic safety analysis. The result of the analysis is that core damage frequency is very low and fulfils this quantitative requirement with high safety margin.  Probabilistic Risk Assessment (PRA) results demonstrate a very low core damage frequency, which meets the goals established for advanced reactor designs, and a low frequency of release due to improved containment isolation and cooling.The predicted core damage frequency (CDF) and large early release frequency (LERF) are lower than the US NRC goals set for new plant designs. The results show the effectiveness of passive systems in mitigating severe accidents and reflect the reduced dependence of the AP1000 NPP on non-safety systems and human actions:   |  |  |  | | --- | --- | --- | | **Summary of AP1000 Plant At-Power PRA Results** | | | |  | **Plant CDF** | **Plant LERF** | | Internal Events | 3.94E-07/reactor-year | 3.83E-08/reactor-year | | Internal Flood | 2.17E-07/reactor-year | 8.40E-08/reactor-year | | Internal Fire | 8.54E-07/reactor-year | 3.42E-07/reactor-year | | Seismic Events | 6.89E-08/reactor-year | 2.83E-08/reactor-year | | **Total During At-Power Events** | **1.53E-06/reactor-year** | **4.93E-07/reactor-year** |  |  |  |  | | --- | --- | --- | | **Summary of Standard AP1000 PRA during Shutdown Events Results** | | | |  | **Plant CDF (per year)** | **Plant LERF (per year)** | | Internal Events | 1.03E-07 | 1.72-08 | | Internal Flood | 3.22E-09 | 5.37-10 | | Internal Fire | 8.5E-08 | 1.43-08 | | **Total During At-Power Events** | **1.91E-07** | **3.20-08** |   The risk associated with the AP1000 plant, as seen before with updated reference plant values, is two orders of magnitude lower than the US NRC safety goal of less than 10E-4 per year for CDF and less than 10E-5/year for LERF. It is also lower than other operating PWRs.  PSA however will need to be updated to account all possible events and site-specific hazards. |
| Article 45 | | |
| The design basis shall incorporate design limits, operational states and emergency conditions, safety classification of SSCs, and significant methods and design assumptions applied in the design and safety assessment. The design basis shall be systematically specified and documented to reflect the actual state of the nuclear power unit. | COM, OR | Design basis of AP1000 NPP are presented in DCD, including design limits, emergency conditions, safety classification of SSCs and methods/assumptions applied in the design and analyses.  Design Basis shall be kept updated by the Owner during plant operation. |
| Article 46 | | |
| The continuous enhancement principle as per Article176, para. 2 shall be applied in relation to the design basis. All reviews shall be carried out by using the deterministic and probabilistic approach to identify the need and possibilities for improvement. | COM | The continuous improvement principle is applied in AP1000 design e.g., based on operating experience, testing and safety analyses. DCD provides several examples how continuous improvement is applied in AP1000 design. |
| Article 47 | | |
| The design limits shall include at least:  1. radiological and other technical acceptance criteria for all operational states and accident conditions;  2. protection criteria for the fuel rod cladding integrity, inclusive of the departure from nucleate boiling ratio, cladding temperature, nuclear fuel temperature, fuel rod tightness (integrity), and maximum allowable fuel damage during all operational states and accidents without nuclear fuel melting;  3. protection criteria for the coolant pressure boundary, including maximum pressure, maximum temperature, thermal and pressure transients and loads;  4. protection criteria for the reactor installation containment structure, including for temperature, containment pressure and allowable containment leak rates, also the necessary margins ensuring its integrity and leak tightness in case of extreme external events, severe accidents and in combinations of initiating events. | COM | Design limits are presented in DCD.   1. For radiological and other technical acceptance criteria, summarized in DCD section 1.2. 2. For fuel and thermal/hydraulic design, see DCD section 4. 3. For coolant pressure boundary, see DCD section 5. 4. For containment, see DCD section 6. |
| Article 48 | | |
| (1) For all operational states and accidents without fuel melt, the NPP unit shall be capable of performing the following fundamental safety functions:  1. control of reactivity;  2. heat removal from the reactor core and the spent nuclear fuel;  3. holding back radioactive substances from spreading into the environment. | COM | AP1000 is capable of performing fundamental safety functions (reactivity control, heat removal and confinement of radioactive substances) in all operating states and accidents without fuel melt. These fundamental safety functions are presented in DCD and confirmed with structural (DCD section 3), deterministic (DCD section 15) and probabilistic (DCD section 19) safety analyses. Spread of radioactivity to the environment is discussed in DCD chapter 12. |
| (2) The NPP design shall include solutions aimed at mitigation of possible radioactive releases into the environment in case of an accident with nuclear fuel melting and the subsequent period, sufficient to maintain the main safety functions as follows:  1. ensure subcriticality of the core to the extent practicable for a long time period and continuously maintain subcriticality in the spent fuel storage pools;  2. ensure residual heat removal from damaged fuel with the help of independent and diversified systems and means, operable in the conditions of such an accident (including one caused by an extreme external event);  3. maintain at all times the "radioactive substance retaining” function. | COM | AP1000 includes technical solutions to mitigate possible radioactive releases into the environment.   1. Ensures subcriticality of the core and spent fuel storage pools (DCD sections 4 and 9). 2. Ensures residual heat removal of damaged fuel with independent and diversified systems, incl. events caused by an extreme external event (see DCD section 6) 3. Ensures that radioactive releases are kept within acceptable limits (see DCD section 6) |
| Article 49 | | |
| (1) In order to specify all events that may have an impact on the safety of the reactor installation and spent fuel storage facility, an initial list of all NPP states shall be developed – steady and transient states, anticipated operating events and initiating events as a result of single or multiple failures of SSCs, human errors, internal and external events and hazards. | COM  OR | The AP1000 plant initiating events, as presented in DCD Chapter 15, for the deterministic safety analyses are classified per ANSI N18.2 [5] classification that divides plant conditions into four categories according to anticipated frequency of occurrence and potential radiological consequences to the public. The four categories are as follows:  • Condition I: Normal operation and operational  transients  • Condition II: Faults of moderate frequency  • Condition III: Infrequent faults  • Condition IV: Limiting faults  DCD Chapter 15 identifies the PIEs evaluated for the deterministic design basis accident analyses and identifies them as Condition II, III, or IV.  Consideration of ‘licensing rule basis’ events that have been required for evaluation by the U.S. NRC, irrespective of their probability of occurrence. Example of these analyses include such elements as the aircraft impact assessment and the treatment of anticipated transients without scram (ATWS) relative to the regulatory requirements in 10 CFR 50.62. It is noted that station blackout is included in the design basis safety analyses and is therefore considered for each initiating event included in the design basis analyses. Internal hazards are presented in the DCD in various sections, such as floods in section 3.4, missiles in section 3.5, pipe breaks in section 3.6 and fires in section 9.  Further considerations may be needed to site-specific external hazards. |
| (2) The selection of multiple failure events shall consider as follows:  1. a postulated common cause failure or inefficiency of all trains of a safety system which performs a required safety function in the conditions of an anticipated operational occurrence or a postulated initiating event;  2. a postulated common cause failure of a safety system or a safety important system performing a main safety function in normal operational mode. | CWO | Common cause failures are considered in AP1000 design by introducing diversified safety functions and SSCs to strengthen the defense-in-depth concept, e.g., diverse means for core cooling, diversity in automatic depressurization and diversity in actuation system.  Common cause analysis is included in the AP1000 plant PRA as stated in the AP1000 plant DCD Section 19.29. The PRA was used to define where and to what degree diversity needed to be incorporated into the AP1000 plant SSCs.  The primary purpose of equipment qualification, as presented in the AP1000 plant DCD Appendix 3D is to reduce the potential for common mode failures due to anticipated environmental and seismic conditions.  The AP1000 plant uses passive safety systems that have a very high reliability. The design PRA considers multiple failures and common mode failures based on the combined probabilities of the initiating event and the reliability of the mitigating features. A total of 791 potential core damage event sequences for internal initiating events at power are modeled in the PRA. DCD Table 19.59-2 provides the contribution of initiating events to core damage and the initiating event frequency. The 19 dominant sequences are given in DCD Table 19.59-3. |
| (3) The accidents with fuel melting in the reactor core and in the spent fuel storage pool that are not practically eliminated (severe accidents) shall be considered in the NPP design basis. Representative severe accident scenarios shall be identified and analysed to specify the boundary conditions for SSCs operation, accident management strategies and the possible safety enhancement measures. | COM | As stated in NPP\_NPP\_000067 [22], The AP1000 plant design features multiple, diverse lines of defense to ensure spent fuel cooling can be maintained for design-basis events and beyond design-basis accidents2. The AP1000 plant lines of defense are:  - During normal and abnormal conditions, defense-in-depth and duty systems provide highly reliable spent fuel pool cooling, relying on offsite AC power or the onsite Standby Diesel Generators.  - For unlikely events with extended loss of AC power (i.e., station blackout) and/or loss of heat sink, spent fuel cooling can still be provided indefinitely:   * Passive systems, requiring minimal or no operator actions, are sufficient for at least 72 hours under all possible loading conditions. * After 3 days, several different means are provided to continue spent fuel cooling using installed plant equipment as well as off-site equipment with built-in connections.   - Even for beyond design basis accidents with postulated pool damage and multiple failures in the passive safety-related systems and in the defense-in-depth active systems, the AP1000 Spent Fuel Pool spray system provides an additional line of defense to prevent spent fuel damage.  Thus, accidents with fuel melting can be considered practically eliminated, existing spent fuel analysis shows that fuel damage frequency (FDF) is orders of magnitude below CDF Core Damage Frequency and Large Release Frequency (LRF). |
| (4) The following shall be considered for design basis specification: possible internal events and hazards such as internal flooding, fires, explosions, and mechanical impacts caused by damaged high-pressure pipelines, impact of missiles from damaged components or loads drop. | COM | AP1000 plant design considers internal hazards as described in DCD 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 Section 9.5.1 – Fire Protection  DCD Appendix 9A – Fire Protection Analysis  PRA Internal Flood – PRA [4] Chapter 56  PRA Internal Fire – PRA [4] Chapter 57 |
| (5) External events and hazards shall be selected according to the requirements of Section IV, Chapter Five. Interrelation and joint consideration of safety with physical protection according to Article 4, para. 1, item 5, shall be taken into account when identifying the external events and the parameters of their impact. | COM  NAS | External events and hazards are considered in the design basis of AP1000 as presented in DCD (e.g., section 3.4 for external flooding, 3.5 for external missiles and 3.7 regarding seismic events).  Further considerations may be needed to ensure that all site-specific external hazards are considered in the design.  Physical protection solutions are considered AP1000 Security Design Report. |
| (6) The design basis shall cover possible combinations of single events, including internal and external hazards that can result in anticipated operational occurrences and accidents without fuel melting. | COM  OR/COM-B | The design basis of AP1000 considers internal and external hazards and combinations of single events.  Internal hazards are considered, such as flood, pipe rupture, equipment failure, and equipment failure generated missiles, and presented in the DCD.  The usual way to consider or screen Initiating Events by External Hazards (and specifically in PRA) is to take into account the combination of external hazards that meet the following.  1. A single event creates the multiple hazard (e.g., a snowstorm which produces high winds and snow drifts).  2. There is dependence between the hazards (i.e., the frequency of the two hazards occurring at the same time is greater than the product of their individual frequencies).  3. Different plant safety functions are affected, OR the effect on one safety function from the combined event is greater than either event individually.  4. The combined hazard does not screen using the individual hazard screening criteria (e.g., the event can happen close enough to the plant to affect it).  Further considerations may be needed to ensure that all site-specific external hazards are considered in the design. |
| (7) The compiled preliminary list of initiating events and NPP states shall be reviewed with the help of a combination of deterministic and probabilistic methods while considering relevant operating experience and safety assessments of other nuclear power plants. The results of research programmes and argumented engineering evaluations shall be additionally considered for the selection of severe accident scenarios. | COM | Deterministic and probabilistic safety analyses are presented in DCD sections 15 and 19. See also response to article 49(1).  Relevant operating experience and safety assessments are considered in the design of AP1000, and they are documented in DCD .  As presented in DCD section 19.59, AP1000 is expected to achieve a higher standard of severe accident safety performance than current operating plants, because both prevention and mitigation of severe accidents have been addressed during the design stage, taking advantage of PRA insights, PRA success criteria analysis, severe accident research, and severe accident analysis. |
| Article 50 | | |
| The final list of events and accidents considered in the design shall cover enveloping scenarios with the lowest margin that meets the acceptance criteria for analysis results in order to define the boundary conditions according to which the safety important SSCs and their functional characteristics will be designed and manufactured. An indicative list of enveloping scenarios and events to be considered in the NPP design, is presented in the attachment to this Regulation. | COM | The list of limiting events and accidents considered in the design are presented in the deterministic safety analysis (see DCD section 15) and probabilistic safety analysis (see DCD section 19).  The AP1000 plant design basis events, as presented in DCD Chapter 15 and as Reviewed for the reference Plant, are identified per the American National Standards Institute (ANSI) N18.2, “Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants” [6] classification that divides plant conditions into four categories according to anticipated frequency of occurrence and potential radiological consequences to the public. The four categories are as follows:  • Condition I: Normal operation and operational transients  • Condition II: Faults of moderate frequency  • Condition III: Infrequent faults  • Condition IV: Limiting faults  The basic principle applied in relating design requirements to each of the conditions is that the most probable occurrences should yield the least radiological risk, and those extreme situations having the potential for the greatest risk should be those least likely to occur.  Internally initiated faults for the AP1000 plant presented in DCD Chapter 15 have been identified by application of the checklist from ANSI N18.2. This document presents a checklist of categorized events that have been identified from assessment of United States (US) nuclear plant Structures, Systems, and Components (SSCs) failure modes and from multiple years of operating experience.  The application of the ANSI N18.2 checklist has been reviewed against the AP1000 plant design and PRA and has been appropriately updated to reflect the plant-specific design features. In particular, design- specific events have been added, such as spurious actuation of the passive residual heat removal (PRHR) system. PIEs are classified into systematic groups per NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants” [7]. For the AP1000 plant safety analyses, AP1000 plant PIEs are assigned to the following NUREG-0800 categories:  • Increase in Heat Removal from the Primary System – DCD Section 15.1  • Decrease in Heat Removal from the Secondary System – DCD Section 15.2  • Decrease in Reactor Coolant System Flow Rate – DCD Section 15.3  • Reactivity and Power Distribution Anomalies – DCD Section 15.4  • Increase in Reactor Coolant Inventory – DCD Section 15.5  • Decrease in Reactor Coolant Inventory – DCD Section 15.6  • Radioactive Release from a Subsystem or Component – DCD Section 15.7  With respect to spent fuel pool cooling, the AP1000 spent fuel pool cooling system is not required to operate to mitigate design basis events. DCD Section 9.1.3.4.3 addresses the event of the loss of cooling by the spent fuel pool cooling system, including failure of a spent fuel pool cooling system pump, leakage from the spent fuel pool cooling system, loss of offsite power and station blackout.  DCD Section 15.8 addresses the Anticipated Transient Without Scram (ATWS) rule 10 CFR 50.62. The ATWS is an anticipated operational occurrence during which an automatic reactor scram is required but fails to occur due to a common mode fault in the reactor protection system. Under certain circumstances, failure to execute a required scram during an anticipated operational occurrence could transform a relatively minor transient into a more severe accident. ATWS events are not considered to be in the design basis for Westinghouse plants. The AP1000 plant includes a diverse actuation system which provides the ATWS Mitigating Systems Actuation Circuitry (AMSAC) protection features mandated for Westinghouse plants by 10 CFR 50.62, plus a diverse reactor scram. Thus, the ATWS rule is met.  DCD Section 1.9.5.1.5 discusses Station Blackout. The NRC has published 10 CFR 50.63 and Regulatory Guide 1.155 which establish requirements so that an operating plant can safety shut down following a loss of all AC power. SECY-94-084 discusses station blackout for passive plants. With respect to Station Blackout, AC electrical power is not needed to establish or maintain a plant safe shutdown condition for the AP1000 plant. Safety-related systems do not need nonsafety-related AC power sources to perform safety-related functions. The Condition II, III, and IV event analyses described in DCD Chapter 15 do not credit AC power for mitigation of the event.  The AP1000 safety-related passive systems automatically establish and maintain safe shutdown conditions for the plant following design basis events, including extended loss of ac power sources. The passive systems can maintain these safe shutdown conditions after design basis events, without operator action, following a loss of both onsite and offsite AC power sources, for 72 hours. DCD subsection 1.9.5.4 provides additional information on long-term actions following an extended station blackout beyond 72 hours.  See also response to article 49(1). |
| Article 51 | | |
| (1) To ensure appropriate reliability, efficiency and independence of the safety important SSCs, the following principles shall be applied in the design:  1. use of practically proven or experimentally tested and qualified components;  2. redundancy of the SSCs dedicated to counteract single initiating events and multiple failure events;  3. diversity of SSCs performing one and the same safety function to protect against common cause failures;  4. fail-safe components to ensure that structures and systems perform their safety functions;  5. physical, structural or spatial separation of safety system trains;  6. functional isolation of interconnected circuits and systems. | COM | Reliability, efficiency and independence of the safety important SSCs are ensured in the design of AP1000 as presented in the DCD.   1. Proven technologies are applied in AP1000 design, and they are complemented with comprehensive testing and qualification activities. 2. The redundancy principle is applied in AP1000 design to counteract against single failures. 3. The diversity principle is applied in AP1000 design to counteract against common cause failures. 4. The fail-safe principle is applied to ensure high reliability of the safety functions. 5. Physical separation, including structural and spatial separation, is applied to ensure high reliability against internal and external events. 6. Functional isolation is applied in the design to ensure independency of the systems. |
| (2) In the design of SSCs important to safety preference shall be given to solutions using inherent safety features (feedback control, thermal inertia and other natural processes). | COM | Inherent safety features are applied in the design of AP1000 as presented in the DCD,  AP1000 design uses extensively inherent safety features including negative feedback coefficients control for power control, thermal inertia, and natural processes.  Thus, AP1000 develops three fundamental safety advances:  1. The AP1000 **plant self-actuates**: For station blackouts, critical systems, structures, and components automatically achieve a fail-safe configuration without the need for operator action or AC/DC power.  2. The AP1000 **plant is self-sufficient**: The passive approach to safety eliminates the importance of AC power and cooling supply.  3. The AP1000 **plant is self-contained**: Systems, structures, and components critical to placing the reactor in a safe shutdown condition are protected within the steel containment vessel which is protected by a robust shield building. |
| (3) The human factor in the design is considered by:  1. automatic or passive devices to actuate and control the safety systems to an extent that does not require intervening of operators for a period of 30 minutes upon the initiating event occurrence;  2. technical features with the help of which to preclude human errors and mitigate their consequences, including during the maintenance of SSCs important to safety. | COM | Human factors are considered in AP1000 design.   1. Passive design solutions and automatic functions are applied in AP1000 design, operator actions are not needed during the first 30 minutes after initiating event. 2. AP1000 design includes features to ensure that human errors will not cause significant risk to safety, e.g., by monitoring, self-surveillance, and other features.   Human factors engineering program is presented in DCD section 18. |
| (4) The failure of normal operation system shall not impede the performance of its designated safety function. | COM | Normal operating systems do not affect the performance of the safety functions. This is considered in the defense-in-depth concept of AP1000, and confirmed in deterministic safety analysis, see DCD section 15 and specific assessment of as part of the Regulatory Treatment of Nonsafety-Related Systems to avoid the Adverse interactions with the AP1000 safety-related systems, including Functional interactions, Spatial interactions, and Human-intervention interactions. |
| (5) Independent performance of the main safety functions shall be ensured for each power unit on multiple-unit sites. | COM | AP1000 plant units at a site are a stand-alone design. There is no sharing of SSCs between multiple units on a site. Hence safety functions of AP1000 are independent from other units in the site. |
| Article 52 | | |
| (1) All SSCs that are important to safety shall be identified and classified in safety classes according to their function and relation to safety. | COM | The AP1000 plant safety classification is a mature methodology applied to the operating AP1000 plants and implements a graded approach such that the structures, systems, and components (SSCs) with the highest safety functions are assigned to the highest safety class.  AP1000 Class A, B, C is assigned to the SSCs with the highest safety importance, for example, the passive safety systems and components that are required to mitigate design basis accidents.  AP1000 Class D is assigned to the active Defense-in-Depth (DiD) SSCs which supplement the capability of the passive systems and to the severe accident mitigation features.  AP1000 Class D SSCs are evaluated by the “Regulatory Treatment of Non-Safety Systems”. The AP1000 plant US licensing basis definition for Class D is consistent with IAEA guidance for “items important to safety". Also, as Class D, AP1000 counts with severe accident mitigation features (due to the low probability of this accidents occurrence, however equipment used to mitigate severe accidents is designed to survive the environmental conditions that the equipment will operate in the severe accident environment for which they are intended).  For the AP1000 plant, the items important to safety, as defined per the IAEA, encompass the Class A, B and C SSCs (“safety-related”) and the Class D SSCs (Defense-in-Depth (DiD) and severe accident mitigation features).  The AP1000 design applies Class A, B, C to passive safety systems and components. Additionally, as safety system support feature, as defined per the IAEA, is the Class 1E DC and Uninterruptable Power Supply System (IDS).  Safety-related structures, systems, and components (SSCs) are credited in the DBE analysis as presented in DCD Chapter 15 and DCD Chapter 6.  Safety classification principles for AP1000 design is presented in DCD section 3.2. |
| (2) SSCs shall be classified by applying the structural approach which is based on a combination of deterministic and probabilistic methods, complemented by engineering assessments where appropriate. | COM | Safety classification principles for AP1000 design is presented in DCD section 3.2. |
| Article 53 | | |
| (1) The process of SSCs safety classification shall cover as a minimum the following steps:  1. systematic identification of functions necessary for the performance of the main safety functions for each operational or accident state;  2. categorization of the specified functions according to their importance to safety by using the results of the safety assessment;  3. specification and classification of SSCs that perform functions characterised as important to safety; the SSCs shall be allocated to safety classes according to the category of the function they perform;  4. specification and classification of other safety important SSCs designed for normal operation. | COM | Safety classification principles for AP1000 design is presented in DCD section 3.2.  The classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements. The classification system provides an easily recognizable means of identifying the extent to which structures, systems, and components are related to ANS nuclear safety classification, NRC quality groups, ASME Code, Section III classification, seismic category, and other applicable industry standards, as shown in DCD table 3.2-3. |
| (2) The functions of SSCs under para. 1, item 2 shall be characterised by the principle of getting the least consequences for the most frequent events and consideration of the following three factors:  1. consequences as a result of a failure to perform a function;  2. frequency of occurrence of the initiating event, combination of events or a common cause failure which require the performance of the respective function;  3. the contribution of the performed function for bringing reactor installation into a controlled or safe state. | COM | Safety classification principles for AP1000 design is presented in DCD section 3.2.  The classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements. The classification system provides an easily recognizable means of identifying the extent to which structures, systems, and components are related to ANS nuclear safety classification, NRC quality groups, ASME Code, Section III classification, seismic category, and other applicable industry standards, as shown in DCD table 3.2-3.  See also assessment for Article 50. |
| (3) Safety-important structures, systems and components for normal operation that are to be considered in the course of classification shall be specified according to their significance for the:  1. protection of personnel and public from the effects of ionizing radiation;  2. prevention of failures that have not been considered in the design basis (including damage of the reactor pressure vessel);  3. decreasing the frequency of SSCs failures that may result in accidents;  4. mitigation of the consequences of external and internal hazards, considered in the design;  5. prevention of initiating events progression in case no other single failures have occurred. | COM | Safety classification principles for AP1000 design is presented in DCD section 3.2.  The classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements. The classification system provides an easily recognizable means of identifying the extent to which structures, systems, and components are related to ANS nuclear safety classification, NRC quality groups, ASME Code, Section III classification, seismic category, and other applicable industry standards, as shown in DCD table 3.2-3.  See also assessment for Article 52 |
| (4) Structures, systems and components under para. 3 shall be directly classified in safety classes according to the consequences of their failure. | COM | Safety classification principles for AP1000 design is presented in DCD section 3.2.  The classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements. The classification system provides an easily recognizable means of identifying the extent to which structures, systems, and components are related to ANS nuclear safety classification, NRC quality groups, ASME Code, Section III classification, seismic category and other applicable industry standards, as shown in DCD table 3.2-3. |
| Article 54 | | |
| (1) Structures, systems and components assigned to safety classes shall be designed, manufactured, installed, tested, operated and maintained in such a way as to ensure the quality and reliability required by the respective safety class. | COM | Safety classification is used as a basis to ensure the required quality and reliability, as presented in DCD section 3.2.2.2. |
| (2) The following shall be specified for each safety class:  1. the appropriate standards and rules for design, manufacturing, installation and inspection;  2. the degree of redundancy, the need for emergency power supply, and qualification for operation under specific adverse environmental conditions;  3. the state of operability or inoperability of SSCs that is considered in the deterministic safety analysis;  4. the applicable quality requirements. | CWO | 1. Safety classification is the basis for the appropriate standards and rules, see DCD section 3.2.2.2. 2. Redundancy criteria/emergency power supply is not directly defined based on the safety class of the component, but single failures, loss of power supply and qualification efforts are considered in the design and analysis to ensure nuclear safety of the NPP. 3. The state of operability/inoperability is considered in deterministic safety analysis, see DCD section 15. 4. Applicable quality requirements related to safety class are summarized in DCD section 3.2. |
| (3) The NPP design shall preclude the interference of individual SSCs important to safety, and shall ensure that a failure of an SSC of one safety class shall not cause a failure of an SSC of a higher safety class. The auxiliary systems, supporting SSCs important to safety, shall be assigned to the same safety class. | CWO | Safety classification principles for AP1000 design is presented in DCD section 3.2.  The classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements.  However, classification of SSCs is slightly different than required in this article, e.g., safety class C includes components, which provides safety support functions to Class A, B and C SSCs. |
| (4) The design shall consider an appropriate isolating device which shall be classified in a higher safety class for the cases of connecting SSCs of different safety classes, or of safety classified SSCs to SSCs that are not safety related. | CWO | Safety classification principles for AP1000 design is presented in DCD section 3.2.  The classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements.  Design includes isolation devices between non-safety classified parts and classified pars, e.g., safety-related systems are connected to the network through gateways and qualified isolation devices so that the safety-related functions are not compromised by failures elsewhere, as presented in DCD section 7.  However, classification of SSCs is slightly different than required in this article, e.g., safety class C includes components, which provides safety support functions to Class A, B and C SSCs. |
| (5) Structures, systems and components that perform different functions shall be allocated to a safety class that corresponds to their most important function. | COM | As presented in DCD section 3.2.2.2, a single item or portion thereof, which provides two or more functions of different classes, is classified according to the most stringent function. |
| Article 55 | | |
| (1) During the design and selection of structural materials of SSCs important to safety, the impact on their characteristics and operational states operability throughout their entire lifetime shall be considered as well as the impacts under accident conditions when the performance of their functions is required. | COM | Selection of materials are based on the safety and seismic classification of the SSCs, as presented in DCD section 3.2. Qualification of components to the normal operation / accident conditions are presented in DCD section 3.10 (seismic qualification) and DCD section 3.11 (environmental qualification). |
| (2) Equipment qualification procedures shall be developed and implemented to confirm that SSCs important to safety will be capable of performing their functions throughout their entire lifetime while considering possible environmental impacts and conditions (seismic impacts, impacts of temperature, pressure, humidity, vibrations, jet blasts, electromagnetic interference, ageing, irradiation and possible combination thereof) in all operational states and accident conditions. | COM | The assessment of the availability of safety-related equipment within these environmental conditions is called “Equipment Qualification” (EQ). AP1000 Equipment Qualification Methodology provides guidelines, acceptable methods, and procedures for the environmental, seismic, and electromagnetic compatibility (EMC) qualification of AP1000® plant safety-related and important-to-safety equipment.  Its basic objective are to:   * + - Reduce the potential for common mode failures due to environmental effects.     - Demonstrate that safety-related equipment is capable of performing its designated safety functions   The assessment of the equipment to perform its function in the severe accident environment is performed through an Equipment Survivability Assessment. See DCD Appendix 19D.  Qualification of components to the normal operation / accident conditions are presented in DCD section 3.10 (seismic qualification) and DCD section 3.11 (environmental qualification), and Appendix 3D . |
| (3) Working conditions of components of structures and systems important to safety shall be simulated by in-situ tests and full-scope tests, or, in the case such tests are practically impossible, alternative methods of proven equivalent effect shall be used. | COM | Qualification of components to the normal operation / accident conditions, including qualification tests and analysis, are presented in DCD section 3.10 (seismic qualification) and DCD section 3.11 (environmental qualification). |
| (4) Basis, methodologies, instructions and results of important to safety SSCs classification and qualification are systematically documented in a way allowing traceability and examination. | COM | SSC classification basis, methodology, instructions, and results are presented in DCD section 3.2. Qualification is presented in DCD sections 3.10 and 3.11. |
| Article 56 | | |
| (1) Severe accident management equipment provided by design shall ensure retaining of the confinement safety function, and include all necessary measures to reliably maintain the integrity and leak-tightness of the containment in its capacity of the last barrier against spreading of radioactive substances into the environment. To this effect, technical means shall be provided for implementation of the following functions:  1. in case of accidents, isolate containment and ensure containment penetrations are leak-tight;  2. control the containment temperature and pressure, including air filtration in case ventilation systems are in place;  3. monitor and control the concentration of explosive gases in the containment;  4. decrease fission products quantity in the containment;  5. diagnose the condition of the fuel in the reactor and the spent fuel pool and provide information for accident management decision-making with the help of measuring devices that are qualified for severe accident conditions. | COM | Severe accident functions are described and analyzed in DCD section 19. Severe accident management equipment is designed to ensure retaining of the confinement safety functions and to include all necessary measures to maintain integrity and leak-tightness of the containment, including functions 1-5 in this article. |
| (2) Nuclear fuel melting shall be prevented in the cases where the isolation of the containment structure cannot be ensured within the required time (in reactor shutdown state and untight containment), or in the cases resulting in containment bypass. | COM | Nuclear fuel melting is prevented to the extent possible in cases when containment isolation is not ensured or in case of containment bypass. |
| Article 57 | | |
| (1) The design of SSCs and other technical features intended to perform safety functions during severe accidents shall implement the following principle requirements:  1. SSCs performing safety functions at other defence-in-depth levels shall be independent to the extent practicable;  2. safety classification, seismic qualification and environmental qualification for the duration of the accident throughout which they are required to remain functional;  3. reliability complying with the performed function, which may require redundancy of active components of the systems and of other engineered and measuring instruments. | CWO  COM | 1. There are SSCs used in Severe Accidents, which are used also in other defense-in-depth levels. However, it is considered a reasonable approach due to the passive safety features of the AP1000 design. Operation of the SSCs during transients does not affect operability during severe accidents. 2. Safety classification rules are defined in DCD section 3.2, seismic qualification rules in DCD section 3.10 and environmental qualification rules in DCD section 3.11. 3. Redundancy principle is applied for active components required for Severe Accidents. |
| (2) Independence of SSCs performing safety functions during severe accidents shall be ensured in terms of adequate power supply (direct and alternating current) for a justified period and considering possible natural phenomena and hazards. | COM | Adequate power supply with autonomy is considered for functions designed for Severe Accidents with consideration of natural phenomena and hazards. |
| (3) The effectiveness, capacity, and qualification of SSCs and the other technical means (including mobile equipment where it is provided) shall be proven and verified. | COM | Severe accident systems are comprehensively analyzed in DCD section 19. Qualification of components are presented in DCD sections 3.10 and 3.11. |
| (4) When the accident management strategy requires the use of mobile equipment, permanent connecting points shall be provided and physical and radiological aspects considered. Appropriate procedures for qualification, maintenance, testing, inspections and personnel training shall be developed for the mobile equipment and the connection lines and points. | COM/OR | Accident management strategy does not rely on mobile connections, but there are mobile connections for back-up to increase nuclear safety, non the less, The AP1000 plant design has the flexibility for the Owner to determine the non‐permanent equipment that is to be available, and its location based on site‐specific conditions and Owner requirements.  For support beyond 7 days, the following potential non‐permanent equipment has been identified:  - Portable diesel generator  - Portable pump  - Diesel fuel oil  - Required hoses, couplings, electrical cabling to connect the offsite equipment  - Communications equipment by hand‐held satellite phones.  For example, a portable engine-driven pump to provide make-up water to PCS tank can be utilized. For those cases, permanent connections are provided, and appropriate procedures and training are applied. |
| (5) The designs of all on-site nuclear facilities shall be reviewed by applying the systematic approach to identify probable dependence on supply of process fluids and power and common servers. It shall be verified that common resources (personnel, technical means, materials) designated for severe accident management, will be sufficient and efficient for each nuclear facility. | COM  OR | Severe accident strategy is presented in DCD section 19, and it is systematically analyzed with PSA.  Sufficient personnel resource is the responsibility of the Owner. |
| (6) Self-sufficiency of on-site nuclear facilities in terms of supplies necessary for safety function performance, shall be analyzed and ensured for a justified period, but not less than 72 hours. | COM | 72 hours self-sufficiency is considered for AP1000 design. After 72 hours, operator actions may be needed to maintain safety of the NPP. Related actions are presented in DCD section 1.9.5.4. |

## CHAPTER 5 - SAFETY ASSESSMENTS

### Section I: General Requirements

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 58 | | |
| (1) Safety assessment is a systematic process that takes place along the life cycle of the NPP in order to determine the fulfilment of all applicable safety requirements of the design, including the extent to which the safety objectives of Article 4 have been met. Design and safety assessment shall be considered elements of a complex iterative process. | OR/COM | Plant Owner is responsible for the SAR document in all stages of the lifetime of the plant.  Westinghouse provides Safety Assessment Inputs .  The standard AP1000 plant safety analysis report is the AP1000 Plant Design Control Document (DCD), APP-GW-GL-700, Rev 19 [2]. The DCD was developed based on the requirements of Regulatory Guide 1.70, “Standard Format and Content of Safety Analyses Reports for Nuclear Power Plants”. The DCD is representative of the content developed for the standard AP1000 plant that is applicable to the development of the Preliminary Safety Analysis Report (PSAR) for future AP1000 units.  The Reference Plant design for future AP1000 units is either Vogtle Unit 3 or Vogtle Unit 4 design. There are design and licensing updates for the Reference Plant design that have occurred since the issuance of the DCD. However, the DCD 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 with requirements related to Preliminary Safety Analysis Report (PSAR) development. The Vogtle Unit 3 and 4 Updated Final Safety Analysis Report (UFSAR) [3] is the United States Nuclear Regulatory Commission approved safety analysis report for the operation of the Vogtle Unit 3 and 4 AP1000 units. It reflects updates to the AP1000 plant since the DCD and site-specific and Owner-specific content for the licensing basis documentation.  See also Assessment on APP-GW-G0R-003 Revision A [23]. |
| (2) Safety assessment shall be carried out during site selection, design, construction, commissioning, operation, implementation of design and operational modifications, periodic safety review and long term operation after the end of the NPP's design life. | OR/COM | Plant Owner is responsible for the SAR document in all stages of the lifetime of the plant.  Westinghouse provides a Safety Assessment Inputs to the Owner which is based on the DCD rev. 19 [2] with applicable changes from the Reference Plant UFSAR [3], and will include applicable updates on a project specific basis. |
| (3) Safety assessment shall be performed on the basis of the results from a safety analysis carried out and additional scientific studies, the analysis of the accumulated operating experience, as well as of the data of approved applied technologies, design solutions and engineering practices. | OR/COM | Safety assessment is carried out based on comprehensive safety analysis (see DCD sections 15 and 19), operating experience (several parts in DCD, see e.g., surveillance requirements or HFE program), scientific testing (see e.g., DCD section 1.5) and engineering practices presented in DCD. |
| Article 59 | | |
| (1) Safety analysis shall be used as a method for assessing the NPP's behaviour in a wide range of operational states and accident conditions, to confirm the adequacy of the design basis and design solutions, and to demonstrate the possibility of maintaining the NPP in a safe state. | EP/OR/COM | Safety Assessment Evaluation is performed by the Nuclear Regulatory Agency.  Safety analyses to confirm design basis are presented in DCD section 15 (deterministic safety analysis) and 19 (probabilistic safety analysis). |
| (2) Safety analysis shall be performed using deterministic and probabilistic methods, while the level of safety achieved by the design shall be justified by a deterministic safety analysis. Probabilistic analysis shall be used in the selection and categorisation of initiating events and accident sequences to complement the information on processes and the behaviour of the NPP, and to assess the contribution of the various safety aspects to the overall safety level. | OR/COM | Safety analyses to confirm design basis are presented in DCD section 15 (deterministic safety analysis) and 19 (probabilistic safety analysis). |
| (3) The results from the safety analysis carried out shall be used to support the integrated decision making process on the NPP safety management. | OR/COM | The results of the safety analysis are used to ensure that design fulfils the safety targets and can be used for decision-making. |
| Article 60 | | |
| (1) The computer programmes and mathematical models of the NPP, used in the safety analysis shall be verified and validated for the respective application and the error of the calculated parameters shall be assessed. Verification and validation data shall be documented as part of the safety assessment. | COM | DCD Chapters 15 and 19 contain the summarization of computer programs and their verification and validation that can be utilized in SAR. Westinghouse provided compliance assessment against the SSR-2/1 document: APP-GW-GL-059 [24]. Summary of the computer codes used for deterministic safety analyses are presented in DCD section 15.0.11. |
| (2) The computer programmes and mathematical models shall be used only in the areas of application for which they have been validated. | COM | Computer programs and mathematical models are used for the purposes for which they have been validated, see DCD section 15.0.11. |
| (3) The input data and mathematical models underlying the safety analysis shall be specific to the plant power unit and reflect the actual configuration of the SSCs. They shall be kept up to date both in the design process and during the operation of the NPP. When updating the data, models and calculations, account shall be taken of new data received, changes to the design and the operational procedures, and advanced methods and means of analysis. | OR/COM | Input data and mathematical models are power plant specific and reflect actual configuration of SSCs.  The Owner shall update Safety Assessment in agreement with the actual status of the Plant. |
| (4) The deterministic and probabilistic safety analysis shall be carried out by experts who have undergone appropriate training to work with the relevant software and who possess the necessary analytical skills, knowledge and experience. | COM | Nuclear safety experts have sufficient skills, knowledge, and experience to perform safety analysis. |
| Article 61 | | |
| (1) Safety assessment shall determine the possibility of deploying the NPP on the selected site on the basis of the following criteria:  1. the scope of research and studies of the processes, phenomena and factors of natural and technogenic origin has been defined;  2. the phenomena and characteristics related to the site and the surrounding area have been adequately identified and taken into account;  3. the characteristics of the population in the area and the possibilities of the emergency plans for the period of operation of the NPP have been analysed;  4. the hazards associated with the site have been identified. | COM  NAS | The site is already selected. The design basis of AP1000 includes comprehensive consideration of internal and external events as presented in DCD.  However, safety assessment may require further consideration of site-specific phenomena’s, characteristics, and hazards to ensure nuclear safety. This will need to be studied considering the recommendations and discussions on references [9], [10]. |
| (2) In determining the hazards related to external events, the effects of the combination of these hazards with the hydrological, hydrogeological and meteorological conditions of the site shall be taken into account. | OR/COM  NAS | The site is already selected.  The design basis of AP1000 includes comprehensive consideration of internal and external events as presented in DCD. DCD Chapter 2 identifies bounding site characteristics and hazards for which the AP1000 plant has been designed. Site-specific reconciliation is performed on a project-specific basis.  Reference plant DCD Table 1.8-2 recognized Identification of Site-specific Potential Hazards as an action required by The Owner.  However, safety assessment may require further consideration of site-specific phenomena’s, characteristics, and hazards to ensure nuclear safety. This will need to be studied considering the recommendations and discussions on references [9], [10]. |
| (3) Design measures for the protection of SSCs, site protection engineering measures or administrative procedures shall be foreseen to ensure an acceptable risk associated with the hazards identified. | COM  NAS | The site is already approved. The design basis of AP1000 includes comprehensive consideration of internal and external events as presented in DCD.  However, safety assessment may require further consideration of site-specific phenomena’s, characteristics, and hazards to ensure nuclear safety. This will need to be studied considering the recommendations and discussions on references [9], [10]. |
| (4) The assessment shall confirm that all relevant factors have been taken into account in the analysis of potential radiological impacts on the population in the area around the NPP in all operational states and accident conditions. | COM  NAS | The site is already approved. The design basis of AP1000 includes comprehensive consideration of design features to minimize potential impacts of radiation.  However, safety assessment may require further consideration of site-specific phenomena’s, characteristics, and hazards to ensure nuclear safety. See also assessment [7]. |
| Article 62 | | |
| (1) All safety functions of NPPs, including civil structures, systems and components, engineering and natural barriers, inherent safety features, as well as human activities necessary to ensure safety, shall be identified and evaluated in the safety assessment. The safety performance assessment shall cover all modes of normal operation (including startup and shutdown), anticipated operational occurrences and accident conditions. | COM | All safety functions, including SSCs, barriers, safety features and human actions are identified in different operation modes and accident conditions and evaluated in the DCD.  Multiple subsections of DCD Chapter 3 identify the plant site-specific features.  DCD Section 3.1 identifies how the AP1000 plant meets the AP1000 design criteria for safety-related SSCs and comply with 10 CFR 50, Appendix A.  Requirement 4 of SSR-2/1 identifies the fundamental safety functions:  1. Control of reactivity  2. Removal of heat from the reactor and from the fuel store  3. Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.  For example, the fundamental safety functions are addressed by equivalent US NRC General Design Criterion, as presented in DCD Section 3.1:  • DCD Section 3.1.3 – Protection and Reactivity Control addresses control of reactivity  • DCD Section 3.1.4, Fluid Systems, Criterion 34 – Residual Heat Removal, Criterion 35 – Emergency Core Cooling address reactor core heat removal  • DCD Section 3.1.2 – Protection by Multiple Fission product barriers address and DCD Section 3.15 Reactor Containment address confinement of radioactive material.  • DCD Section 3.1.6 addresses fuel and reactivity control |
| (2) The assessment of safety functions shall determine whether the reliability of their implementation is consistent with their importance to safety, which requires assessment of the reliability and qualifications of the SSCs entrusted with the performance of these functions, their vulnerability to single failures and common cause failures, and the application of the principles of redundancy, diversity, independence, isolation and physical separation. | COM | Comprehensive structural (DCD section 3), deterministic and probabilistic safety analysis (DCD sections 15 and 19) are performed to ensure that initiating events or component failures do not cause nuclear safety risk. Application of nuclear safety principles, such as redundancy, diversity, functional isolation, physical separation, autonomy, are applied in the AP1000 design as presented in DCD. Qualification activities are presented in DCD sections 3.10 and 3.11. |
| Article 63 | | |
| (1) The assessment of the application of the defence in depth concept shall confirm that account has been taken of the possible initiating events at the respective levels of the defence in depth and that the main safety functions defined in Article 48, para. 1 have been fulfilled. | COM | Comprehensive safety analyses are performed to demonstrate that all possible initiating events are considered, and fundamental safety functions presented in Article 48 para 1, are available, see DCD section 3 for structural analyses, section 15 for deterministic safety analyses and section 19 for probabilistic safety assessment.  The DCD as a whole demonstrates that the concept of defense in depth is applied in the AP1000 plant design. US NRC design criteria that are equivalent to the criteria in paras. 2.21 to 2.18 of SSR-2/1 are explained in DCD Section 3.1. Westinghouse provided compliance assessment against the SSR-2/1 document: APP-GW-GL-059 [24] with additional information.  DCD Chapter 6, 9, 15, and 19 provide additional supporting information.  EPS-GW-GL-701 [25] discusses in more details the AP1000 plant compliance with the concept of defense in depth. |
| (2) The assessment of the implementation of the defence in depth concept shall determine whether sufficient measures are in place to ensure:  1. detection and prevention of deviations from normal operation;  2. cessation of the development of anticipated operational occurrences related to safety;  3. control and management of the accidents within the limits established by the design basis;  4. practical elimination of large or early releases of radioactive substances into the environment;  5. limiting in terms of time and place of the radiological impacts of nuclear fuel meltdown accidents that have not been practically eliminated. | COM | Comprehensive safety analyses are performed to demonstrate the strength of the defense-in-depth concept, see DCD section 3 for structural analyses, section 15 for deterministic safety analyses and section 19 for probabilistic safety assessment.  Practical elimination of large or early releases of radioactive substances is considered in the AP1000 design and assessed in separate report “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5]. |
| (3) The independence of the levels of defence shall be assessed by an appropriate combination of deterministic and probabilistic safety analysis and engineering judgement. For each initiating event (starting at level 2), the SSCs required to meet the objectives of par. 2 shall be identified, and in the safety analysis, it shall be demonstrated that SSCs designed to function at a single level of defence are sufficiently independent from the SSCs provided for the other levels of the defence in depth. | COM | Comprehensive safety analyses are performed (DCD sections 15 and 19) to demonstrate the strength of the defense-in-depth concept. |
| (4) The safety assessment shall examine the necessary physical barriers to the proliferation of radioactive substances and technical measures to protect the barriers and preserve their effectiveness. This process shall include an assessment of:  1. safety functions that must provide protection for the barriers;  2. the potential threats to their implementation;  3. the mechanisms of occurrence of these threats;  4. measures to prevent the occurrence of such mechanisms;  5. measures to mitigate the consequences of failure of a safety function;  6. assessment of the sufficiency of the barriers. | COM  NAS | Safety assessment include assessment of physical barriers, see DCD Section 3.1.2 Protection by Multiple Fission product barriers, and fuel (DCD Chapter 4), reactor coolant system (DCD Chapter 5), containment (DCD Chapter 6).  Safety assessment includes description of safety functions, which protect physical barriers and threats to the physical barriers, such as internal and external hazards, which are considered in the design. Site-specific external hazards may need to be further considered in the safety assessment.  Comprehensive safety analyses are performed to assess the sufficiency of the barriers and mitigation mechanisms to minimize the nuclear safety risks related to the threats, see DCD section 3 regarding structural analyses, section 15 regarding deterministic safety analysis and section 19 regarding probabilistic safety assessment. |
| (5) The safety assessment shall address the measures foreseen in the design to detect failures or bypass at each level of defence in depth. Particular attention shall be paid to internal and external events and hazards that could adversely affect more than one barrier or cause simultaneous failures of safety systems. | COM  NAS | Comprehensive safety analyses are performed to assess the sufficiency of the barriers and mitigation mechanisms to minimize the nuclear safety risks related to the threats, see DCD section 3 regarding structural analyses, section 15 regarding deterministic safety analysis and section 19 regarding probabilistic safety assessment.  Site-specific external hazards may need to be further considered in the safety assessment. |
| Article 64 | | |
| The safety assessment shall be intended to determine the sufficiency of the safety margins foreseen in the design under normal operation, anticipated operational occurrences and accident conditions. | COM | Safety assessment presented in the DCD, and related safety analysis and tests, which are done to AP1000 design, is used to ensure that there are sufficient safety margins in normal operation, AOOs and accident conditions.  Therefore, for each of the deterministic safety analyses presented in DCD Chapter15, the US NRC acceptance criteria and/or other analysis criteria is presented, as well as the results of the analysis, therefore the margin to acceptance criteria is presented. Individual analysis descriptions identify key input and assumptions.  DCD Section 15.0.3 identifies the initial conditions assumed in the accident analyses. |
| Article 65 | | |
| (1) Assessment of the radiation protection measures shall be carried out for all operational states and accident conditions. Radiation protection measures at the operational states shall aim at achieving the following objectives:  1. limit exposure doses of the personnel and the public below the adopted statutory limits;  2. maintain radiation doses at the lowest possible level. | COM | See BGP-GW-GL-202 [7] for the Assessment on the Bulgarian Regulation on Radiation Protection.  ALARA-principle is applied in the AP1000 design to ensure that radiation protection measures are sufficient and doses to the personnel and public remain as low as reasonably achievable (see DCD section 12).  Radiation shielding is provided to ensure that necessary emergency operations can be performed (see DCD section 12.3.2). |
| (2) The adequacy of the design protection measures in case of accident conditions shall be assessed in the light of the safety objectives under Article 4 related to limiting the duration and place of implementation of the measures for protection of the public. | COM | See BGP-GW-GL-202 [7] for the Assessment on the Bulgarian Regulation on Radiation Protection.  Radiological analyses are performed in DCD section 15, to ensure that there are sufficient design solutions to ensure that radiological releases in accidents are kept below the acceptable limits. |
| (3) The assessment shall confirm that sufficient technical and organisational measures have been envisaged to provide defence in depth of all sources of ionising radiation at the NPP, to monitor the radiation parameters of SSCs, the premises, the site and the monitored area, and to control the personnel exposure. | OR/COM | See BGP-GW-GL-202 [7] for the Assessment on the Bulgarian Regulation on Radiation Protection  Radiological analyses are performed in DCD section 15, to ensure that there are sufficient design solutions to ensure that radiological releases in accidents from all sources of ionizing radiation are kept below the acceptable limits.  DCD section 12 provides technical solutions for radiation protection, including radiation monitoring systems in DCD section 12.3.4 and health physics facilities in DCD section 12.5. |
| (4) The assessment shall determine the correctness of the input data and the validity of the methodology used to calculate exposure doses of the personnel and population. | OR | Offsite dose calculations are responsibility of the Owner. |
| (5) Subject to assessment shall be design measures for provision of sufficient space for inspection and maintenance, use of automated repair tools and non-destructive testing in high radiation areas, measures preventing spread of contamination, and the fulfilment of sanitary rules for protection of the personnel. | COM | DCD section 12 provides assessment of technical solutions to fulfill ALARA principle, including sufficient space reservations for inspection and maintenance, provisions to remotely operate, repair, service, monitor or inspect equipment and personnel protection. |
| Article 66 | | |
| (1) The following aspects shall be taken into account when assessing the loads on the SSCs due to external and internal impacts as a result of operational states and accident conditions:  1. loads and load combinations for structures and components consistency with their safety class;  2. expected frequency of occurrence of each load or load combinations;  3. stresses and deformations in structures and components with a safety class for the loads and load combinations specified;  4. Individual and cumulative degradation of structures and components, taking into account possible degradation mechanisms (plastic deformation, fatigue, ageing and their potential interaction). | COM | 1. Loads and load combinations are considered for structures and components based on their safety class, see DCD section 3, e.g., DCD section 3.8 for structures. 2. Expected frequencies for different initiating events and hazards are evaluated in probabilistic safety analyses, see DCD section 19. 3. Stresses and deformations to the structures and components are evaluated in DCD section 3, e.g., related to mechanical systems and components in DCD section 3.9. 4. Degradation mechanisms are considered in the AP1000 design and safety assessment, e.g., for piping see DCD appendix 3B.2. |
| (2) The total number of anticipated transients over the operational time and their frequency of occurrence shall be assessed on the basis of available documented data, operating experience, requirements of the operating organisation and site characteristics. | COM  NAS | DCD subsection 3.9.1.1 Design Transients provides an assessment of Mechanical Systems and Components design transients. The impact of Earthquake Cycles can be seen in DCD subsection 3.7.3.2.  The frequency of the initiating events is evaluated in connection of probabilistic safety analysis, see DCD section 19. This evaluation includes review of pressurized water reactor (PWR) operating experience, past PRAs, and consideration of AP1000-specific features.  Site specific characteristics and related external hazards may require further considerations. |
| Article 67 |  |  |
| The safety assessment shall confirm that the SSCs important to safety are provided in the NPP by a proven and conservative design that has considered the following engineering aspects:  1. where applicable, the operating experience, including the results of the analysis of the root causes of operational events, has been taken into account;  2. an appropriate classification and qualification system of the SSC has been developed and implemented, reflecting the importance of the performed safety functions, the severity of the consequences of their failure and the operability during anticipated operational occurrences and accident conditions;  3. the industry standards and design standards used for design, manufacture and construction ensure:  (a) the ability of the SSCs to perform the assigned functions, taking into account the manufacturing tolerances of the components, the accuracy of measurement of the parameters and the time delay of the control signals;  (b) the ability of the SSCs to perform the assigned functions with low failure rate in accordance with safety analyses;  (c) the ability of the SSCs to perform assigned functions under operational loads or loads caused by postulated initiating events;  4. the materials used are appropriate for the purpose with regard to the specified standards and the conditions that arise as a result of operational states and accident conditions considered in the design;  5. where practicable, the safe failure principle has been applied or means of failure detection have been provided for;  6. the effects of ageing and wear, as well as life-limiting factors such as cumulative fatigue and embrittlement, have been taken into account;  7. the necessary instructions and procedures defining the actions of personnel during normal operation, in case of deviations from the operational limits and conditions, in case of anticipated operational occurrences and in case of accidents are available and ensure an adequate level of safety. | COM | Proven and conservative design is applied for AP1000 design.   1. Operating experiences are utilized in AP1000 design, see e.g., DCD subsection 1.9.5.5 Operational Experience for Operational Experience considered in the Design or technical specifications in DCD section 16. 2. Safety and seismic classification are presented in DCD section 3.2, qualification principles are presented in DCD sections 3.10 and 3.11. 3. Safety classification is used as a basis to define adequate codes and standards for the SSCs, as presented in DCD section 3.2. 4. Materials are used based on specified standards and accident conditions, see qualification basis in DCD sections 3.10 and 3.11. 5. Fail-safe principle is applied in AP1000 design, e.g., in PHRH HX, CMT, PCS and containment isolation are initiated by operation of fail-safe valves. 6. Aging mechanisms are considered in the AP1000 design by proper qualification activities (see DCD section 3.10 and 3.11 and appendix 3D) 7. Necessary instruction and procedures are specified during construction of the plant. Principles are defined in DCD section 13. |
| Article 68 | | |
| (1) The design solutions used in NPP evolution designs shall have been approved in previous applications at existing NPPs. Where this is not possible, safety shall be justified by use of results from ancillary research programmes or by the operating experience gained in other relevant applications. | COM | The AP1000 plant is designed to achieve a high safety and performance record. The AP1000 Nuclear Power Plant (NPP) is a two-loop, 1,110 MWe class pressurized water reactor (PWR) is conservatively based on proven PWR technology which builds on over 60 years of PWR operating experience, but with an emphasis on safety features that rely on natural forces.  Selection of proven components has been emphasized to ensure a high degree of reliability with low maintenance requirements. Component standardization reduces spare parts, minimizes maintenance, reduces training requirements, and allows shorter maintenance durations. Built-in testing capability is provided for critical components.  The design of the major components required for power generation such as the steam generators, reactor coolant pumps, fuel, internals, turbine and generator is based on equipment that has successfully operated in power plants. Modifications to these proven designs were based on similar equipment that had successful operating experience in similar or more severe conditions.  The latest design and analysis techniques, including computer codes, are used in the AP1000 design and analysis. In most cases, these are the same as used in support of current plant uprates and steam generator and reactor vessel head replacements. Previous Westinghouse experience and expertise allows confidence that the requirements for plant life will be met. Major primary components of the AP1000 plant are designed for 60 years and are adaptations of current proven technology to ensure design life and function.  Plant construction techniques are based on proven approaches, including the extensive use of modules, which have been demonstrated in successful large construction projects, both nuclear and non-nuclear.. |
| (2) Based on the results and conclusions of the operating experience, the safety analysis and the research conducted, the necessity and the benefit of improvement of the design beyond the established practice shall be reassessed. When introducing innovative or unapproved design solutions, compliance with safety requirements shall be demonstrated through a suitable ancillary programme for preliminary experimental testing and confirmation of the relevant features. | COM | The design solutions used in AP1000 are based on previous application of AP600 and operating experiences received from the existing NPPs, see e.g., DCD sections 1.5 and 1.6. The results from operating experience, safety analysis, research, testing etc., are utilized to improve the design and they are described in the DCD. |
| Article 69 | | |
| The safety assessment shall systematically take into account human factors and man-machine interaction in the design of the NPP. For this purpose the following shall have been ensured:  1. identify the actions assigned to operating personnel to ensure safety and perform analyses of the tasks in making operational decisions ;  2. provide sufficient information and management tools to enable the operating staff to:  (a) manage and control normal operation;  (b) easily assess the NPP's overall condition under normal operation, anticipated operational occurrences and accident conditions;  (c) control the state of the reactor and the state of all SSCs;  (d) identify changes in the condition of NPP that are important to safety;  (e) confirm the implementation of the intended automatic actions;  3. design working areas and the operating conditions so as to take into account the ergonomic principles and allow reliable and efficient task performance;  4. the NPP design is tolerant to human error to the extent practicable;  5. all operating actions that have to be performed for a short time and are automated;  6. sufficient and reliable communication means are in place between the Main Control Room/Emergency Control Room, local control panels and Emergency Response Centre. | COM | DCD section 18 presents human factors engineering program, which is applied to ensure that items 1-6 in this article are fulfilled. Human errors are analyzed in deterministic and probabilistic safety analyses (DCD sections 15 and 19). |
| Article 70 | | |
| (1) The safety assessment shall identify possible interactions among the NPP systems, between the NPP and other off-site industrial sites, and among the plant power units on the same site. Interactions among systems shall be taken into account in all operational states and accident conditions, including external hazards. | COM  NAS | Safety assessment includes consideration of interfaces between NPP systems in normal operation and accident conditions.  Further considerations may be needed in the safety assessment to site-specific characteristics and hazards. |
| (2) The assessment shall take into account not only the physical interaction but also the effects from operation, maintenance, failures or malfunctions of a system on the operating conditions of another system important to safety. Interactions between systems belonging to different levels of defence in depth shall be avoided by means of appropriate design solutions. | COM | Safety assessment includes consideration of interfaces between NPP systems in normal operation and accident conditions. Defense-in-depth principle is applied in the AP1000 design. |
| (3) The Grid - NPP interaction shall be subject of evaluation in order to ensure the reliability of power supply to the systems that are important to safety. | COM | DCD section 8 presents grid – NPP interface. Deterministic and probabilistic analyses are performed (DCD sections 15 and 19) to assess that there is reliable power supply to the systems and components important to safety. Additional description of AP1000 Unit and Gird Interaction can be found in APP-GW-G0R-006 [26]. |
| (4) In case of extreme weather conditions or in case of an external hazard affecting more than one power unit on-site, the capabilities to fulfil the safety function for a reasonable period of time shall be assessed of the common plant support systems, residual heat removal systems and ultimate heat sink. | COM  NAS | The design basis of AP1000 includes comprehensive consideration of external events as presented in DCD, see e.g., consideration of external flooding in section 3.4, external missiles in section 3.5 and seismic events in section 3.7.  However, safety assessment may require further consideration of site-specific phenomena’s, characteristics, and hazards to ensure nuclear safety. |
| Article 71 | | |
| (1) The operating organisation shall carry out an independent review of the safety assessment prior to using it or submitting it for regulatory review. The independent review shall be carried out by suitably qualified and experienced experts who have not participated in the safety assessment process. The scope of the independent review shall include:  1. a comprehensive review of the completeness of the safety assessment and the way in which it is implemented and presented;  2. a detailed overview of individual aspects of the safety assessment that have the greatest impact on safety;  3. review of the models and data used in the safety analysis in terms of their up-to-dateness, representativeness and relevance. | OR | Requirement for the Owner.  Independent Review of the Safety Analysis is a Bulgarian Regulatory Requirement. |
| (2) The design basis, the safety assessment and the technical and organisational measures ensuring the implementation of the defence in depth concept shall be documented in a preliminary, interim and final safety analysis reports related to the authorisation process under the SUNEA. | OR/COM | Design basis and related safety assessment is documented to the safety analysis report. Safety assessment report is updated during the project lifecycle. |
| (3) The Safety Analysis Report shall confirm the fulfilment of safety requirements and shall be used to support safe operation, including during assessment of the consequences to safety from design modifications and operational practices. | OR/COM | Safety Analysis report confirms the fulfilment of the safety requirements and supports safe operation of the plant. |
| (4) The operating organisation shall maintain the Safety Analysis Report updated in accordance with the changes made to the SSCs important to safety, the assessments and analyses carried out and the current safety requirements. The report shall be timely updated when there is new safety assessment information, including one regarding the site and NPP siting area characteristics. | OR | Requirement for the Owner. |

### Section II: Deterministic Safety Analysis

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 72 | | |
| (1) A deterministic safety analysis, including neutron, thermohydraulic, radiological, thermo-mechanical and strength calculations, shall be performed to determine the behaviour of the reactor installation and the spent fuel storage pool for events and states specific to the NPP. | COM | Deterministic safety analysis is summarized in DCD section 15. Strength calculations are presented in DCD section 3. |
| (2) The NPP events and states defined in the design basis shall be grouped and analysed in separate categories with different acceptance criteria under Article 47 in order to demonstrate that the events with the highest frequency have no off-site radiological consequences, and events with potential consequences are very unlikely and fulfil the safety objectives under Article 4, paras 3 and 4. Depending on the expected frequency of occurrence and potential consequences, the following categories shall be distinguished:  1. steady and transient states during normal operation;  2. anticipated operational occurrences;  3. accidents without nuclear fuel melting;  4. accidents with nuclear fuel melting. | COM | NPP events are grouped and analyzed in separate initiating event groups depending on the frequency of the even (see DCD section 15.0.1).  Deterministic safety analyses are summarized in DCD section 15. Accidents with fuel melting are considered in DCD section 19. |
| (3) In the category of steady and transient states during normal operation, modes specific of the unit shall be analysed, such as: startup; power operation; hot standby; hot shutdown; cold shutdown; refuelling; heating and cooling at maximum permissible speed; step load changes; load changes at different power ranges; reducing power from full load to house-load; boundary states defined by the operating limits and conditions. | COM | As presented in DCD section 15.0.1.1, Normal operation, and operational transients (condition I) includes events that are expected to occur frequently or regularly in the course of power operation, refueling, maintenance, or maneuvering of the plant. |
| (4) In the category of the anticipated operational occurrences, transients specific to the power unit shall be analysed, such that are typically associated with loss of operational and/or standby power supply, turbogenerator/turbine trips, failures in the instrumentation and control systems, loss of one or several main coolant pumps. | COM | As presented in DCD section 15.0.1.2, Faults of Moderate Frequency (Condition II) includes events that, at worst, result in a reactor trip with the plant being capable of returning to operation. |
| (5) In the accidents without nuclear fuel melting category, individual postulated initiating events and multiple failure initiating events specific to the unit shall be analysed, including those resulting from internal and external hazards, from common cause failures and events that potentially affect all the nuclear facilities on the site. | COM  NAS | As presented in DCD sections 15.0.1.3, Infrequent Faults (Condition III) and section 15.0.1.4 (Limiting Faults), they cover events that may occur infrequently during the life of the plant (Condition III) and faults, that are not expected to take place, but are postulated because their consequences include the potential of the release of significant amounts of radioactive material (Condition IV).  Multiple failures, including common cause failures together with initiating event, may require further considerations in the deterministic safety analyses. |
| (6) By means of the safety analysis it shall be demonstrated that accidents with nuclear fuel melting that lead to large or early releases of radioactive substances into the environment have been practically eliminated. | COM | The Deterministic Safety Analyses show through their acceptance criteria that no core melt will occur under the conditions specified in them Including: Departure from Nucleate Boiling Ratio (DNBR), Peak Clad Temperature, Peak Fuel Enthalpy, or in case of a Loss of Coolant Accident 10 CFR 50.46 Criteria(Peak cladding temperature < 2200 F (1205ºC), Maximum local cladding oxidation < 17% thickness, - Core-wide hydrogen generation < 1% of zinc surrounding active fuel length, Core coolable geometry maintained,- Long-term core cooling provided).  Accidents with fuel melting are evaluated in DCD section 19. Furthermore, separate report has been prepared regarding practical elimination, see report “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5]. |
| (7) The states which have to be practically eliminated shall be determined taking into account:  1. initiating events which lead directly to a severe accident with large or early releases (destruction of major components such as the reactor pressure vessel);  2. dependent failures, internal and external events and hazards with the potential to cause large or early releases;  3. fuel meltdown scenarios that endanger the integrity of the containment;  4. fuel meltdown in a spent fuel storage pool (even when it is inside the containment) in view of the impossibility to practically implement accident management measures. | COM | Accidents with fuel melting are evaluated in DCD section 19.  Furthermore, separate report has been prepared regarding practical elimination, see report “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5]. |
| (8) For the accidents involving fuel meltdowns, that can not be practically eliminated, it shall be demonstrated that the off-site radiation impact is limited and implementation of long-term measures for protection of the population are not necessary in accordance with the safety objective under Article 4, para. 4. | COM | AP1000 design includes severe accident strategy to manage events involving fuel meltdowns which cannot be practically eliminated, presented in DCD section 19. |
| (9) Any elimination of an initiating event or accident sequence from the safety analysis shall be justified and documented on the grounds of compliance with technically valid criteria. | COM | Initiating events or accident sequences, which are eliminated, are justified, and documented in the safety analysis report. |
| Article 73 | | |
| (1) The deterministic safety analysis shall confirm the design basis of the NPP for the particular site and NPP siting area. | COM  NAS | DCD section 15 provides deterministic safety analysis and confirms the design basis of the NPP.  Site-specific hazards may require further considerations in the safety assessment. |
| (2) The deterministic analysis shall demonstrate the possibility of controlling anticipated operational occurrences through the instrumentation and control systems, and individual initiating events through the automated action of the safety systems. When analysing such events a safety margin shall be ensured by applying a conservative approach and the following general rules:  1. determine the initial and boundary conditions with reasonable conservatism;  2. apply the most unfavourable, independent of the initiating event, single failure of an active or passive component performing a safety function (or a single personnel error) with the most adverse effect on the evolution of the event;  3. consider an additional failure (sticking) of the most effective control rod, conservatively identified with respect to the reactor scram efficiency in hot state;  4. consider operability of only the safety classified SSC, qualified to operate under the conditions of the particular event;  5. consider such an efficiency of a safety classified SSC that leads to the most adverse consequences;  6. consider the operability of the normal operation systems only if the effect of their operation degrades the consequences of the event;  7. consider as part of the postulated event any failure occurring as a result of the initiating event;  8. consider operator's actions taken no earlier than 30 minutes after the beginning of the event;  9. consider uncertainties through appropriate conservative assumptions, confidence factors, parameters sensitivity analysis, or uncertainty assessment. | COM | Deterministic safety analysis (DCD section 15) demonstrates how AOO’s are managed with I&C. Table 15.0-6 summarizes the plant systems and equipment available for transients. As presented in section 15.0.1.1, a conservative set of initial conditions are applied for Condition I transients.   1. Principles for initial conditions applied in the analysis is summarized in 15.0.3.2 and more in detail in the specific analyses. Summary of initial conditions is presented in DCD table 15.0-2. Boundary conditions applied in the analysis are presented in the specific analysis in DCD section 15. 2. Principles how limiting component failures (incl. human errors) are considered is summarized in 15.0.12. Single failures assumed in the analyses, is presented in table 15.0-7. 3. The most effective control rod sticking fully withdrawn is considered in the deterministic safety analysis (see DCD section 3.1.3, GDC 27) 4. Only safety-classified SSC are needed to operate under the conditions of the particular initiating event (see DCD table 15.0-6). Non-safety classified systems can be used to mitigate consequences (see DCD table 15.0-8). 5. Principles how limiting component failures (incl. human errors) are considered, is summarized in 15.0.12. 6. Normal operating systems are not credited in the analyses. Only if they degrade the consequences of the event, then normal operation systems are considered. 7. Consequential effects of the initiating event are always considered in the analysis. 8. Operator actions are not considered before 30 minutes after the initiating event as presented in the analyses. 9. Conservative assumptions are used in the analyses to ensure that there are high safety margins to manage the events. |
| (3) Multiple failures events analyses shall be conducted to confirm the capability of the design to deal with common cause failures, to determine the need for additional measures to prevent the melting of nuclear fuel, and to demonstrate sufficient margin to the occurrence of cliff-edge effects. In analysing these events, the following general rules shall apply:  1. use moderately conservative or realistic assumptions, hypotheses and arguments that are reasonable for the purpose of analysis;  2. use the conclusions and results of the probabilistic safety analysis;  3. consider failures and events that may occur in all operating states;  4. consider the geographic and spatial location of the NPP, the capacity and diversification of the SSCs performing safety functions, and the feasibility of implementing the actions envisaged for accident management;  5. adequately consider the uncertainties and their impact on the end. | COM  NAS | Multiple failure events are considered in probabilistic safety analyses, see DCD section 19. Multiple errors are also considered in the deterministic safety analyses, e.g., related to the failure of automatic depressurization.  However, further considerations may be needed in deterministic safety analyses to confirm sufficient capabilities of the design with multiple failure events.  See response in Article 87 for the impact of Cliff edge effects in the design. |
| (4) Analyses of accidents with fuel meltdown and the radiological consequences thereof shall be made using a realistic approach and reasoned assumptions, applying the following requirements to:  1. consider scenarios which may occur in all operational states;  2. consider successful actions of the personnel and the accident management teams;  3. use the conclusions and results of the probabilistic safety analysis levels 1 and 2, and the applicable experimental data;  4. consider the characteristics of the phenomena arising from severe accidents and the associated uncertainties;  5. determine the possibilities for interaction with other nuclear facilities on the site. | COM | Fuel meltdown analyses are considered in DCD section 19.   1. Representative phenomenological issues related to severe accident conditions are presented in DCD section 19.34. 2. Consideration of personnel actions are considered in the analysis. 3. Results from probabilistic safety assessment with applicable experimental data is utilized in the analysis. 4. Characteristics of the phenomena are considered in the analyses. 5. Design does not include shared systems with other nuclear facilities on the site. |
| Article 74 | | |
| The evolution of the accident sequences shall be predicted and analysed until reaching predefined end states of the NPP for each category of events, including low power events and shutdown state of the reactor installation. | COM | The analyses are performed until controlled state is reached, including low power and shutdown states, see DCD section 15. |
| Article 75 | | |
| (1) An analysis of the radiological consequences shall be performed for all operational states and accident conditions in order to assess the effectiveness of the protective barriers, determine the need to implement measures to protect the population in case of accidents, and assess the time available for their implementation. | COM  OR | Analysis of radiological consequences are presented in DCD section 15.  Off-site radiological analyses are in the responsibility of the Owner. |
| (2) The assessment of the radiological situation for all operational states shall be carried out applying probabilistic distribution of the parameters of atmospheric dispersion that are typical for the area of the NPP siting. | COM | Atmospheric dispersion factors are presented in DCD chapter 15, appendix A. |
| (3) The assessment of the radiological consequences from accident conditions shall take into account the most adverse weather conditions typical for the area of the NPP siting. The consequences shall be determined for different periods of accidents evolution (related to the avertable dose intervention levels) considering all the mechanisms of migration of radioactive substances into the environment and all exposure pathways. | COM  OR | Analysis of radiological consequences is presented in DCD section 15.  Off-site radiological analyses are in the responsibility of the Owner. |
| Article 76 | | |
| The deterministic analysis of internal and external events and hazards shall determine the effectiveness of safety functions, taking into account event specific features. The level of detail of the analysis shall be consistent with the contribution of the event to the overall risk for the NPP, the number of physical barriers it threatens, and the possibility of the event causing simultaneous failures of safety systems. | COM  NAS | Internal and external hazards are considered in the design of the nuclear island structures to ensure that plant can be safely shutdown. DCD section 15 presents initiating events with detailed consideration of effectiveness of the safety systems and failure considerations.  Site-specific hazards may require further considerations in the safety assessment. |
| Article 77 | | |
| (1) To justify the effectiveness and the adequacy of the fire protection measures, a deterministic analysis of the fire risk shall be made by experts with qualification and experience both in the analysis of process systems and in the field of fire safety. | COM | Appendix 9A of DCD presents fire protection analysis. |
| (2) The analysis under para. 1 shall be performed for all steady states and transient processes at normal operation considering the following assumptions:  1. occurrence of a single fire and its spread in each zone containing highly flammable materials;  2. dependent failures in the affected areas as a consequence of the fire;  3. combined effect from the fire and another initiating event which is likely to occur irrespective of the fire. | COM | Appendix 9A of DCD presents fire protection analysis, including fire spreading, dependent failures and combined effects. |
| (3) The results of the fire hazard analysis shall indicate the possible consequences of the fire and the operation of the fire detection and fire suppression systems, including potential failures and spurious actuation. | COM | The basic principle for AP1000 design is that fire detection and suppression systems are not needed for reaching a controlled state in case of a fire. However, there is separate automatic suppression features assessment included as a part of fire hazard analysis. Potential failures and spurious actuations are considered in the fire hazard analysis as presented in Appendix 9a of DCD. |
| Article 78 | | |
| (1) The deterministic safety analysis shall be carried out according to the methodologies developed in advance, which shall include the assumptions of the analysis and their basis, the individual implementation steps and justified criteria for the acceptability of the results. | COM | Deterministic safety analysis, including analysis basis, methodologies, assumptions, analysis steps and justified criteria, are summarized in DCD section 15. |
| (2) The methodologies for analysis, the results of the safety analysis and the conclusions regarding the fulfilment of the acceptability criteria shall be documented in a verifiable and traceable way, paying special attention to the cases when engineering judgement have been used. | COM  NAS | Methodologies, results, and conclusions of the analysis are summarized in DCD section 15.  Documentation of engineering judgement in the safety analysis may need to be further considered. |

### Section III: Probabilistic Safety Analysis

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 79 | | |
| (1) For the application of an integrated approach to the NPP safety assessment, a Probabilistic Safety Analysis (PSA) shall be performed that systematically identifies all factors which have a significant contribution to safety and the radiation risk to the population and the environment. The PSA shall be conducted at the following levels:  1. Probabilistic Safety Analysis Level 1 – it identifies the accident initiating events, and the accident sequences, and assesses the nuclear fuel damage frequency;  2. Probabilistic Safety Analysis Level 2 – it identifies possible radioactive substances release pathways into the environment and assesses the large radioactive releases frequency;  3. Probabilistic Safety Analysis Level 3 – it assesses the risk to human health and other social risks such as soil, water and food contamination by radioactive substances, and it is implemented by a decision of the Chairperson of the Nuclear Regulatory Agency. | COM, COM-B | PSA has been widely used during AP1000 Design Phase and used to optimize design decisions and optimization.  The design Probabilistic Risk Assessment (PRA), which is also called design Probabilistic Safety Analysis (PSA), for the standard AP1000 plant is documented in APP-GW-GL-022 Revision 8. AP1000 Design 19 provides a good summary of PSA use in its section 19.59.3.9.  Vogtle Units 3 & 4 counts with a specific and Peer- Reviewed PRA that has been developed implementing updates to the AP1000 plant design from the standard AP1000 plant design to the Vogtle Unit 3 & 4 design and site-specific aspects of the Vogtle 3 & 4. AP1000 units. This has been upgraded to ASME/ANS-RA-Sa 2009, NRC-endorsed this by Regulatory Guide 1.200.  The updated Vogtle Unit 3 &4 PRA is for at-power risk and is limited to Level 1 and Level 2 analyses for Internal Events, Internal Flood, Internal Fire and Seismic. A qualitative External Hazards Analysis was performed based on the Vogtle Units 3 & 4 plant- and site- specific information. Additionally, a Shutdown Defense-In-Depth (DID) model was developed following NUMARC 91-06, EPRI TR-1013501 and EPRI TR-1016231 methodology. This qualitative shutdown DID risk assessment is intended to support the requirements of Article (a)(4) of 10CFR50.65. The shutdown DID model includes evaluations of key safety functions applicable to low power and shutdown conditions to support the development of the shutdown critical safety function status tree for the identified plant operating states.  The updated Vogtle Unit 3 & 4 PRA will serve as the basis to support the PSAR, for Kozloduy plant project.  Further considerations may be needed to cover all events, including site-specific external hazards, and Site-Specific Level-3 Analysis, in the Probabilistic Safety Assessment. |
| (2) A probabilistic safety analysis shall be implemented in order to achieve the following objectives:  1. perform a systematic analysis of the compliance with the main safety objectives and criteria, assess the frequency of occurrence of severe fuel damage and large radioactive releases into the environment, and determine the risk to the population;  2. prove, where possible, a sufficient margin until cliff-edge effects occur. | COM  COM-B | Objectives of the PSA are presented in the DCD section 19.1.2.  Further considerations may be needed to:  - Systematic analysis (all important factors needs to be considered, including site-specific hazards)  - Consideration, that sufficient margins for cliff-edge effects are provided. See repose in Article 87 for the impact of Cliff edge effects in the design |
| (3) The scope of PSA shall include:  1. significant sources of radioactivity (nuclear fuel in the reactor core and the spent fuel pool) and all operational states of the power unit (including operation at full power, low power and shutdown state);  2. all significant initiating events, internal hazards (such as internal fires and floods) and external events and hazards (such as seismic impacts and extreme weather conditions) identified on the basis of appropriate selection criteria;  3. all functional dependencies resulting from spatial distribution and other possible causes for common cause failures;  4. realistically modelled behaviour of the power unit, taking into account the actions of the operating personnel in accordance with the operating and emergency procedures and justified time for the performance of the functions of the systems;  5. human error analysis, taking into account the factors which can influence the performance of the personnel in all operational states and accident conditions.  6. sensitivity analysis of results and uncertainty assessment. | COM  COM-B | 1. All operating states are considered, as presented in DCD section 19.1.3. An update of Spent Fuel PSA may be needed for spent fuel pool assessment, and some other scopes (COM-B). 2. PSA (DCD section 19) includes a comprehensive set of initiating events and hazards. Further considerations may be needed to cover all events, including site-specific external hazards, in the Probabilistic Safety Assessment. 3. Common cause failure analysis is performed to identify and model the dependencies. Physical separation and related common cause failures are considered in the PSA hazard analysis. 4. Realistic modelling of the NPP behavior is considered in the PRA, with the consideration of operating personnel and justified time for the performance of the functions and systems, see DCD section 19.1.3 for PSA methodology. 5. Human reliability analysis is provided in DCD section 19.30. 6. Sensitivity analysis is provided in DCD section 19.50 and uncertainty assessment in DCD section 19.51. |
| (4) The probabilistic safety analysis shall be performed using unit-specific data and in accordance with a contemporary proven methodology. The data, methodology and results of the analysis shall be documented in a traceable way and kept up-to-date in accordance with the operating organisation's management system. | COM-B  OR | Data, methodology and results of PSA is provided in DCD section 19.  Further considerations may be needed to consider site-specific data in the PSA analysis.  Owner is responsible to maintain up-to-date PSA analysis during the operation. |
| Article 80 | | |
| (1) The probabilistic safety analysis shall have the necessary quality and level of detail for using the obtained results in support of the deterministic analysis when making decisions in the process of designing and operating the NPP with respect to:  1. demonstrating a balanced design in which there is no an initiating event which has a disproportionate impact on the overall risk of the NPP;  2. identifying the need for changes to the design and operational practices and assessing the adequacy of the proposed safety improvement measures;  3. assessment of the operating limits and conditions, emergency procedures and severe accident management guides;  4. assessment of the significance of the operational events;  5. development and validation of personnel training programmes, including full-scope simulator training scenarios;  6. assessment of the maintenance, surveillance and testing programmes for SSCs having a significant contribution to risk. | COM/OR  NAS | Probabilistic safety analysis is performed in good quality and high detail, reference plant PRA to be used as base is counted with a specific and Peer-Reviewed PRA that has been developed implementing updates to the AP1000 plant design from the standard AP1000 plant design to the Vogtle Unit 3 & 4 design and site-specific aspects. This has been upgraded to ASME/ANS-RA-Sa 2009, NRC-that was endorsed by Regulatory Guide 1.200.  Further considerations may be needed to include some additional scopes from the reference plant e.g., to cover all possible external hazards, site-specific topics.   1. Balanced design is demonstrated based on the results of the PSA (section 19 of the DCD) 2. AP1000 design improvements based on PSA studies are presented in DCD section 19.1.6.2. 3. Assessment of operating limits and conditions, emergency procedures and SAMG are performed during construction phase. 4. PSA results are provided in DCD section 19.59. 5. Validation of personnel training programmes is an owner requirement. Westinghouse can provide support as discussed in APP-GW-G0R-010 [31] 6. Assessment of maintenance, surveillance and testing programmes are performed during construction phase. |
| (2) For using the PSA results, the limitations of the analysis performed shall be identified. Each specific application shall be checked against the identified limiting factors and the impact of sensitivity and uncertainty of the results. | COM | Uncertainties and limitations of the PSA are presented in DCD sections DCD sections 19.50 and 19.51. |
| (3) When using the PSA to assess the requirements for periodic tests and the admissible system or component downtime, the analysis shall consider all the states of that system or component and the safety function that they perform. | OR/COM | Reliability of AP1000 SSCs will be ensured by means of the application of Operational Phase Reliability Assurance Activities (OPRAAs), which are contained in various operating plant programs.  The OPRAAs are composed of site administrative, maintenance, operational, and testing programs to enhance operational phase reliability throughout the designed plant life. The following reliability assurance programs are credited as OPRAAs:  • Maintenance Rule Program, per requirement in 10 CFR 50.65 (or equivalent process), which uses Probabilistic Safety Assessment Insights.  • QA Program  • In-service Testing Program  • In-service Inspection Program  • Technical Specifications Surveillance Test Program  • AP1000 Plant Short-Term Availability Controls Program  • Site Maintenance Program  Requirements for periodic testing and system/component downtime based on PSA are performed during construction of the NPP. |
| (4) Where the PSA results indicate importance to safety for certain components, their reliability and operability shall be ensured and documented in the safety analysis report. | COM | PSA results indicate importance of the components (DCD section 19.59) and they are part of the safety analysis report.  The AP1000 D-RAP Program provides additional details for the risk determination process. All SSCs identified as risk significant via the D-RAP are included within the initial Maintenance Rule (MR) scope as High Safety Significance (HSS) Structures Systems and Components (SSCs) |
| (5) The external events analysis shall take into account the impact of the external hazard on the reliability of the buildings and civil structures, the robustness of the systems and components and the possibilities for human action under such conditions. | OR/COM-B | External events analysis is presented in section 19.58 of DCD.  Further considerations may be needed for site-specific external events. |

### Section IV: Analysis of External Events and Hazards

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 81 | | |
| To assess the effectiveness and adequacy of the NPP protection against external events, the design shall consider and assess all sources of hazard that may affect safety originating from:  1. natural phenomena, processes and factors characteristic of the site and the surrounding area;  2. hazards induced by human activity. | COM/COM-B/OR | DCD Chapter 2 identifies external hazards addressed in the AP1000 plant design.  AP1000 DCD Subsection 19.58 provides guidelines for an owner to prepare the external hazards report and thus, this action has been recognized as the responsibility of owner.  External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3), external missiles (section 3.5), and malevolent aircraft impact (appendix 19F).  Site-specific hazards may require further considerations in the safety assessment. |
| Article 82 | | |
| The assessment of external events shall include the following methodological steps:  1. identification of all sources of hazard specific to the NPP site and area of the NPP siting;  2. preliminary screening based on established criteria;  3. assessment of the impact parameters of the selected external events;  4. analysis of external events using deterministic and probabilistic methods. | COM  NAS | Site is already approved [19].  External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  . |
| Article 83 | | |
| (1) Identification of the external events of natural origin characteristic of the site and the area around it shall be carried out taking into account geological, seismotectonic, meteorological and hydrological processes, phenomena and factors, biological phenomena, natural forest fires as well as interrelated processes and phenomena (such as earthquakes and floods, fires, tsunami, land subsidence, collapse, etc.). The completeness of the list of identified external events shall be justified and well-grounded. | COM  NAS | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Identification of Hazards was performed to obtain site approval order.  However, site-specific hazards may require further considerations in the safety assessment. |
| (2) The preliminary screening of the events is based on criteria established with conservative assumptions. Excluding events from a follow-up assessment and analysis shall be allowed only in cases in which it has been demonstrated with a high degree of confidence that it is physically impossible or extremely unlikely that the event could affect the safety of the NPP. External events of natural origin which, in combination with other events, may affect the safety of NPP shall not be excluded from the analysis. | NAS | Identification of Hazards was performed to obtain site approval order.  External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  However, site-specific hazards may require further considerations in the safety assessment. |
| (3) The impact assessment of the selected events of natural origin shall be made using a deterministic approach and probabilistic methods with respect to the analysis of the available data and deducing a dependency between the severity of the event (intensity and duration) and the frequency of excedance. The following rules shall apply when assessing the impact parameters:  1. the assessment shall be based on all available site and site location data, including historical data;  2. external events that change with time (climatic and other changes) shall be taken into account;  3. well-grounded methods and assumptions shall be used and the natural and model uncertainties affecting the results of the assessments shall be analysed;  4. the confidence intervals shall be determined of the assessments of the intensity of impacts (the most probable severity of the event). | COM  NAS | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  However, site-specific hazards may require further considerations in the safety assessment. |
| (4) Based on the assessment under para. 3, the events of natural origin considered in the design shall be grouped for analysis in the following categories:  1. design-basis events that include single events of natural origin and combinations of causal or unrelated phenomena and processes whose frequency of occurrence is at least 10-4 per year. Where it is not possible to determine the frequency of occurrence with an acceptable confidence level, the design-basis event shall be selected and justified in such a way as to ensure an equivalent level of safety;  2. extreme events which are identified, assessed and analysed in order to define the margins to cliff-edge effects. | COM, COM-B  NAS | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Site-specific hazards may require further considerations in the safety assessment. See repose in Article 87 for the impact of Cliff edge effects in the design. |
| (5) The impact parameters of each design-basis event shall be determined conservatively, taking into account the results of the assessment of the relevant processes and phenomena. The design-basis events shall be compared with the relevant historical data to see if historical extreme events have been exceeded with a sufficient margin. | COM  NAS | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Site-specific hazards may require further considerations in the safety assessment, including extreme hazards. |
| (6) Based on the deterministic analysis of design-basis events, a robust concept of protection shall be developed that shall provide for conservative implementation of the main safety functions for all direct and possible indirect effects of the design-basis event. The concept of protection shall:  1. use moderate conservatism to ensure the design safety margin;  2. be based primarily on passive measures, where applicable;  3. ensure that accident management measures remain effective during and after the design-basis event;  4. take into account the evolution of the event over time and the possibility of forecasting;  5. ensure that procedures and means for checking the state of the NPP are in place along with alarms and annunciation during and after the design-basis event which shall be enacted upon the occurrence of predefined limit parameters;  6. consider the fact that the event may cause multiple failures in the safety systems and/or their supporting systems and may simultaneously threaten multiple power units at the same site, site infrastructure, regional infrastructure and external supplies;  7. ensure that sufficient resources are available on multi-unit NPP sites, taking into account the use of plant common equipment (including mobile) and maintenance;  8. not adversely affect protection against design-basis events of other origin. | COM  OR/COM-B | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Site-specific hazards, as investigated by the owner, may require further considerations in the safety assessment. This will need to be studied taking into account the recommendations and discussions on references [9], [10]. |
| (7) The structures, systems and components identified as part of the concept of protection against design-basis events shall be assigned to a safety class and qualified for the conditions and impacts of the relevant natural phenomena and hazards. To qualify for seismic impacts, SSCs are subdivided into seismic categories according to their functions for ensuring safety during and after an earthquake. In terms of Safe Shut-down Earthquake (SSE), the minimum acceleration for seismic assurance shall be 1 m/s2 at the natural terrain elevation, while the response spectrum shall be at least equal to the corresponding response spectrum for conventional buildings construction. | COM-B | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Regarding seismic impact, seismic design response spectra is presented in DCD section 3.7.1.1 fulfilling this requirement. Seismic categorization principles are presented in DCD section 3.2.  Response spectra need to be developed for the project. See recommendations in reference [10].  Site-specific hazards may require further considerations in the safety assessment. |
| Article 84 | | |
| (1) Accidents with nuclear fuel melting as a result of external events of natural origin leading to large or early releases of radioactive substances into the environment shall have to be practically eliminated, by proving with a high degree of confidence that occurrence of such events is extremely unlikely. | COM | Practical elimination is evaluated in report “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5]. |
| (2) Extreme events and phenomena, which are more severe than the design-basis ones, but can not be practically eliminated, shall be identified and analysed with a realistic approach in order to practically identify the possible improvements related to them. The assessment process shall take into account the following aspects:  1. determination of the event impact parameters in case of which the main safety functions performance can not be ensured;  2. demonstration of a sufficient margin until cliff-edge effects.  3. identification of the most robust means of ensuring the main safety functions;  4. the possibility that the event may cause multiple failures in the safety systems and/or their supporting systems and may simultaneously threaten multiple power units on the same site, site infrastructure, regional infrastructure and external supplies;  5. provision of sufficient resources for multi-unit NPP sites, taking into account the use of plant common equipment or services;  6. conducting field checks and walkdowns. | CWO  NAS | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Site-specific hazards may require further consideration in the safety assessment.  See response in Article 87 for the impact of Cliff edge effects in the design. |
| Article 85 | | |
| (1) Determination of the external events of technogenic origin, characteristic of the NPP site and the siting area, shall be carried out taking into account the following sources of hazard:  1. biplane crash of a modern passenger aircraft;  2. external fires (caused by off-site sources);  3. explosions caused by off-site or on-site sources, but outside the buildings with SSCs important to safety;  4. release of poisonous or suffocating gases or chemical substances stored on-site or off-site;  5. release of radioactive substances from off-site sources;  6. transportation and industrial activities near to the site;  7. electromagnetic off-site radiation;  8. combinations of the above sources as a result of a common initiating event. | OR/ COM-B | 1. Aircraft crash is considered in Appendix 19F of the DCD.   Items 2-8 in this article may require further site-specific considerations in the safety assessment. This will need to be studied taking into account the recommendations and discussions on references [9], [10].  For Aircraft Crash Assessment see article 33(5). |
| (2) The preliminary screening of external events of technogenic origin shall take place in two stages. Screening criteria based on the distance from the source of hazard to the NPP shall be used at the first stage, and at the second stage - the annual frequency of occurrence; | N/A | Site is already approved by Bulgarian Nuclear Regulatory Agency Order No. АА-04-30. 21.02.2020. By which BNRA Approves: "the site selected by KOZLODUY NPP – NEW BUILDS PLC (UIC 202058513) for the siting of a nuclear facility - nuclear power plant (Site No. 2) with a location, boundaries and characteristics according to the submitted documents"[19]. |
| (3) The assessment of the frequencies and impact parameters of events of technogenic origin shall be carried out similarly to the events of natural origin and aim at defining the categories of the design-basis events and the extreme events. | N/A | Site is already approved by Bulgarian Nuclear Regulatory Agency Order No. АА-04-30. 21.02.2020. By which BNRA Approves: "the site selected by KOZLODUY NPP – NEW BUILDS PLC (UIC 202058513) for the siting of a nuclear facility - nuclear power plant (Site No. 2) with a location, boundaries and characteristics. Events have already being considered by the owner and approved by BNRA. according to the submitted documents"[19]. Events have already being considered by the owner and approved by BNRA. |
| (4) The approaches to analyse events of technogenic origin, acceptance criteria and protection concepts shall be determined depending on the category of the event, its specificity and its safety consequences. | NAS | Further considerations may be needed for site-specific external hazard assessment. |
| Article 86 | | |
| (1) In pursuance of the safety objective under Article 4, para. 3, the NPP design shall take into account the consequences of a modern passenger airplane crash (as a technogenic event in the category of extreme events). The analysis shall demonstrate the assurance of the main safety functions that render and maintain the NPP in a safe state. | COM-B | Aircraft crash is considered in Appendix 19F of the DCD. Methods described in NEI 07-13, Revision 7 (Reference 1) were followed to assess the effects on the structural integrity of the primary containment and spent fuel pool, and to assess the physical, fire, and vibration effects of the aircraft impact on the core cooling capability of the existing and enhanced design.  For Aircraft Crash Assessment see article 33(5). |
| (2) The design measures for the protection of the systems necessary for rendering and maintaining the NPP in a safe state following the impact of the plane crash, and the civil structures in which they are located shall consider the effects of:  1. direct and secondary impacts on their mechanical toughness;  2. vibrations on their operability;  3. ignition and explosion of aviation fuel on their integrity. | COM | Aircraft crash is considered in Appendix 19F of the DCD. Methods described in NEI 07-13, Revision 7 (Reference 1) were followed to assess the effects on the structural integrity of the primary containment and spent fuel pool, and to assess the physical, fire, and vibration effects of the aircraft impact on the core cooling capability of the existing and enhanced design.  For Aircraft Crash Assessment see article 33(5). |
| (3) Civil structures or individual parts thereof containing nuclear fuel or SSCs performing key safety functions shall be capable of preventing penetration of aviation fuel therein. Aircraft fuel-induced fires shall be considered as different types of combinations of fireball and fiery surface. Secondary fires occurring as a result of the main fire shall also be considered. | COM | Aircraft crash is considered in Appendix 19F of the DCD. Methods described in NEI 07-13, Revision 7 (Reference 1) were followed to assess the effects on the structural integrity of the primary containment and spent fuel pool, and to assess the physical, fire, and vibration effects of the aircraft impact on the core cooling capability of the existing and enhanced design.  For Aircraft Crash Assessment see article 33(5). |
| (4) Consequence analysis shall be carried by:  1. using a realistic approach, taking into account the best characteristics of input materials, realistic assumptions about failures and modern analytical methods;  2. not considering other concurrent failures of SSCs and the NPP;  3. assessing the sensitivity of the results for confirming availability of a sufficient margin until cliff-edge effects occurrence. | COM  NAS | Aircraft crash is considered in Appendix 19F of the DCD. Methods described in NEI 07-13, Revision 7 (Reference 1) were followed to assess the effects on the structural integrity of the primary containment and spent fuel pool, and to assess the physical, fire, and vibration effects of the aircraft impact on the core cooling capability of the existing and enhanced design.   1. Realistic approach is considered in the analysis in accordance with methodology. 2. No additional failures of SSCs considered. 3. Additional considerations may be needed for cliff-edge effects occurrence in the safety assessment.   For Aircraft Crash Assessment see article 33(5). |
| (5) The protection concept shall take into account the impact of the event on the ability of the personnel to perform the necessary actions and the possibility of external supplies. | COM | Consideration of personnel ability to perform tasks is considered in the methodology report NEI 07-13 (e.g., related to fire safety).  For Aircraft Crash Assessment see article 33(5). |
| Article 87 | | |
| (1) The following aspects shall be taken into account when assessing the impact parameters and the analysis of external events of natural and technogenic origin and when defining the concepts of protection:  1. attentive use of generalised conditional probabilities of failure in view of failure mechanisms differences in one and the same type of NPP;  2. considering the large uncertainties in the parameters of the events in the assessment of the margins to cliff-edge effects occurrence;  3. considering the impact of external events both on systems and components, and on the dependability of buildings and civil structures;  4. the possibility of limiting the impact of external events through a suitable site master-plan (particularly important for multi-unit NPP sites or power units belonging to different generations). | COM  NAS | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Site-specific hazards and may require further consideration.  AP1000 Passive design provides and enhanced assurance that small deviations in plant parameters will not give rise to large variations in plant conditions (Cliff Edge Effects). The passive safety systems will continue to work at parameters values that exceed those considered in the design.  The limiting values of parameters considered for design are limits that are not to be exceeded to ensure the accomplishment of safety functions, as designed. These parameters are selected with enough conservativeness and margin.  However it should be noted that in the case of some of these design values were beyond their limits, AP1000 taking into account the passive safety features of the design, will not suffer a complete loss of its safety functions but a progressive deterioration of these passive safety systems performance (e.g. less heat been rejected to a hotter environment as Ultimate Heat Sink, or more probability of failure of some components), thus no cliff edge effects are determined. Thus, AP1000 has design has made additional evaluations to determine some of the margin that is embedded in the existing design. Some examples of resistance to these phenomena and margins are described below.  **Seismic Resistance**  The seismic design of plant SSCs is described in DCD Sections 3.7. The standard plant is conservatively designed to protect the plant against design basis safe shutdown earthquake with a peak ground acceleration (pga) of 0.3g. As part of the detailed design, site specific reconciliation analysis, or equipment qualifications, the site-specific earthquake can be used to justify relaxing seismic requirements if necessary. The Reference Plant seismic ground design response spectra are based on Regulatory Guide 1.60 spectra that have been enhanced to include the high frequency characteristics of the Eastern United States.  In addition to the design basis seismic analysis, the AP1000 plant nuclear island is evaluated for a seismic margin assessment which extends to 67 percent above the SSE design basis PGA of 0.3g. This larger seismic event is referred to in the U.S. as the RLE, which has a PGA level for the AP1000 plant of 0.5g. A more detailed discussion of the seismic margin assessment is provided in section 19.55 of the DCD. For the AP1000 plant, seismic margin analyses demonstrate that the critical SSCs have a high confidence of a low probability of failure (HCLPF) level for seismic events equal to or greater than the RLE level. The “high confidence” is defined as 95 percent probability for SSCs to maintain their structural integrity and function, while the “low probability” is, at most, 5 percent. For Containment structures these are above 0.7g.  **External Flooding Resistance**  The plant is designed so the site is dry considering the probable maximum flood is defined on a site-specific basis to bound site-specific external hazards. such as river flooding, upstream dam failure, tsunami, or other natural causes.  Design and protection feature against external flooding are further discussed in Section 3.4 of the DCD. What differentiates the AP1000 design from other plants relative to external flood protection is the ability of the plant to cope with flood levels that exceed the maximum probable site flood. The margin is directly Attributable to the following key features:  1. Safe shutdown and core cooling are provided by systems located inside the containment vessel, and thus protected from flooding.  2. That these systems are designed to “fail safe” upon loss of power, loss of I&C controls, or loss of instrument air.  The AP1000 plant provides margin beyond the design basis flood to maintain a safe shutdown condition with no fuel damage or radiological releases to the public for extreme flood levels. The AP1000 plant can perform these functions after the postulated loss of all on-site AC (and DC) power sources with minimal operator actions in the first 72 hours. Margin above the site grade flooding level has been evaluated to be at least equivalent to a water level of one floor.  **Extreme Temperatures**  Unique to the AP1000 plant design is the use of the steel containment vessel with cooling from the Passive Containment Cooling System (PCS). This provides a path for the removal of decay heat from the containment atmosphere to the environment as the safety-related ultimate heat sink. The AP1000 plant has been designed so that an extreme ambient temperature within the design basis will not prevent the delivery of key safety functions, however some analyses have been performed for higher temperatures than those stated as the maximum design safety temperatures. The maximum and minimum external design temperatures are 46,1°C (115°F) and -40°C (-40°F) respectively.  The design PRA [4] has demonstrated a very low core damage frequency and a very low large release frequency with the inclusion of conservative assumptions made in specifying the success criteria of the passive systems, which demonstrates margin to avoid cliff-edge effects. See design PRA [4] Chapter 33 (Fault Tree and Core Damage Quantification) and Chapter 43 (Release Frequency Quantification). See DCD Section 19.59 for a summary description of results.  The AP1000 design is extremely robust to loss of makeup capability, which de-emphasizes the consequences of external events compromising the connection of the plant to the makeup sources located outside containment and the auxiliary building. No off-site resources requirement is expected for at least 7 days to mitigate postulated severe accident consequences. In general, Westinghouse recommends that each unit should have at least two locations where they can get small portable electrical generators and self-powered pumps which could be used via connecting with the safety-related connections included in the design.  Additionally, the AP1000 accident management program involves additional guidelines for the conditions which the external hazards are more severe than those considered in the design and accident management is required for extended period of times (+72 hours). |
| (2) The results of the external events analysis shall be considered in the design, in the operational and maintenance procedures of the SSCs which ensure the fulfilment of the main safety functions as well as in the training programmes of the personnel and the emergency response teams. | COM  NAS | External hazards are considered in DCD, e.g., in section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  Site-specific hazards may require further considerations. |

## CHAPTER 6 – REQUIREMENTS FOR DESIGN OF NPP AND PLANT SYSTEMS

### Section I: General Requirements

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 91 | | |
| (1) SSCs important to safety shall ensure safe shutdown of the reactor and maintaining it subcritical, cooling of the reactor coolant boundary, residual heat removal, confinement of the radioactive substances within the prescribed limits for the operational states where applicable, for accidents without fuel melting, and for the impacts caused by internal and external events considered in the design. | COM  NAS | Deterministic and probabilistic safety analysis demonstrates that SSCs important to safety can shutdown the reactor and maintain it safety state.  Radiological limits and consideration of site-specific external hazards may require further considerations in the safety assessment. |
| (2) In accidents with fuel melting, SSCs important to safety shall be able to ensure the performance of the "confinement of radioactive substances" function; to that end they shall ensure and maintain the function of "residual heat removal" from the damaged fuel, and containment cooling. The spent fuel pools shall be maintained subcritical at all times, and the reactor core - in the long-term aspect. | COM | Severe accident strategy is presented in DCD section 19. the severe accident mitigation features of the AP1000 passive plant that are designed to minimize any radiological impact from hypothetical accidents resulting in extensive damage to the nuclear fuel in the reactor core. Severe accident management capabilities have been integrated into the AP1000 plant design from the beginning of the design process. PRA [4] and the associated analyses and testing were used to identify scenarios, boundary conditions and postulated severe accident phenomena that must be mitigated to ensure containment integrity in the event of core damage.  In Severe Accidents, SSCs important to safety are able to ensure confinement of radioactive substances functions, including heat removal from the damaged fuel and containment. Spent fuel pools and reactor core are maintained subcritical.  The AP1000 plant maintains one consistent philosophy for the operator to mitigate severe accident scenario: depressurize the RCS and send coolant, by whatever means available, as close to the core as possible to protect all fission product barriers from failure. The plant passive design features facilitate a single path of recovery and operator actions, if needed, to mitigate the event to ensure that heat removal is provided through active DiD or passive safety‐related sources of water inventory designed to remove heat from the core, the containment, and the spent fuel [12].  The AP1000 design provides flexible, consistent, diverse, and redundant levels of defense (passive and active) against the release of radioactivity to the environment following core damage. Severe accident phenomena are addressed with engineered design features to reduce the impact of phenomenological uncertainties. The AP1000 plant’s severe accident features promote RCS depressurization, in‐vessel retention of molten core debris, and recovery of the damaged core within the reactor vessel. Hydrogen that may be produced by cladding oxidation during the core melting and relocation is managed by providing engineered release locations, passive mixing into a large containment volume, intentional ignition at low concentrations and passive recombination. |
| (3) For the performance (or restoration) of the required safety functions during accident with fuel melting, both stationary systems and mobile equipment located on the NPP site can be considered in the design. | COM | Severe accident strategy is presented in DCD section 19 including the SSC required for severe accident management. |
| Article 92 | | |
| (1) SSCs important to safety, their structure, layout and operational condition shall provide possibility for testing, maintenance, repair, inspection and control, over the whole plant operating lifetime, without significant reduction in their functional availability. When SSCs important to safety cannot undergo in-service testing and inspection to a sufficient extent to detect potential failures, their reliability shall be ensured by another proven alternative method, or the design shall conservatively consider a higher failure rate. | COM | Passive features are applied in AP1000 design to achieve high reliability. Testing has been performed to confirm the operation of new AP1000 plant features as discussed in the AP1000 plant DCD Section 1.5. Pre‑operational tests performed in the plant are discussed in Chapter 14. Periodic in-service tests are discussed in the AP1000 plant DCD Sections 3.9 and 16.1.  Maintainability of the AP1000 plant was assessed as part of the human factor assessment presented in the AP1000 plant DCD [2] Chapter 18. The AP1000 plant layout has taken into consideration required access for testing, maintainability, repair, replacement and in-service inspection of components.  Testing, maintenance, repair, inspection, and control during lifetime of the plant without significant reduction in the functionality, is considered in the AP1000 design. |
| (2) SSCs important to safety shall be designed, located and protected in a way that leads to reducing the rate and consequences of fire. The design options shall ensure the performance and maintaining of the main safety functions and control of the power unit condition. | COM | Fire safety principles are considered in AP1000 design and detailed fire safety analyses are performed (DCD section 9, appendix 9A) to ensure that main functions are available.  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 Section 9.5.1.2.1.2, Fire Detection and Alarm Systems)  - Provide the capability to extinguish fires in any plant area, to protect site personnel, limit fire damage, and enhance safe shutdown capabilities  - Supply fire suppression water at a flow rate and pressure sufficient to satisfy the demand of any automatic sprinkler system plus 500 gpm for fire hoses, for a minimum of 2 hours  - Maintain 100 percent of fire pump design capacity, assuming failure of the largest fire pump or the loss of offsite power  - Following a safe shutdown earthquake, provide water to hose stations for manual firefighting in areas containing safe shutdown equipment |
| Article 93 | | |
| The safety systems shall operate so that any initiated actuation shall lead to complete fulfilment of the safety functions. Resetting of the safety systems to their initial state shall require consecutive actions of the operating personnel. | COM | Safety systems actuation is designed to lead to complete fulfilment of the safety function. Resetting of the safety systems (e.g., reactor trip circuit breakers) to their initial state requires operator actions (see. e.g., DCD section 7.2.2.2.7). |
| Article 94 | | |
| (1) The NPP site shall be provided with facilities for personnel protection in case of an accident. They shall be located, protected and equipped so as to ensure habitability and personnel protection over a specified period of time. | OR/COM | Emergency response facilities (see DCD Non-System Based Design Description chapter 3.1) and control rooms are designed to ensure habitability and personnel protection |
| (2) The design shall foresee at least one emergency response centre where the technical support teams for the operating personnel during accident shall operate, and where the emergency recovery activities on the NPP site shall be coordinated. | OR/COM | See DCD Section 1.9.3, Three Mile Island Issues The AP1000 plant provides for an onsite technical support center and operational support center.  The offsite emergency response facility is the responsibility of the Owner/Licensee. |
| (3) The emergency response centre shall be physically separated from the main control room (MCR) and shall be suitably laid out, designed and protected, so as to preserve its functionality, habitability, and efficiency under the accident conditions that are to be managed (inclusive of severe accident and extreme external events of natural origin). | OR | The offsite emergency response facility is the responsibility of the Owner/Licensee.  See DCD Section 1.9.3, Three Mile Island Issues The AP1000 plant provides for an onsite technical support center and operational support center.  Emergency response facilities includes technical support center (see DCD Non-System Based Design Description chapter 3.1). which is physically separated from the main control room. Functionality, habitability, and efficiency of emergency response facilities are considered as part of HFE design (see DCD section 18).  Technical Support Center, Mission and Major Tasks: The mission of the technical support center (TSC) is to provide an area and resources for use by personnel providing plant management and technical support to the plant operating staff during emergency evolutions. The TSC relieves the reactor operators of peripheral duties and communications not directly related to reactor system manipulations and prevents congestion in the control room. The TSC is located in the control support area (CSA) of the Annex Building.  Communications needs are established for the staff within the TSC, and between the TSC and the plant (including the main control room and operational support center), the emergency operations facility, the License, the outside authorities and the public.  The design includes adequate shielding as discussed in Chapter 12. Adequate space, resources and access is provided for maintenance, emergency equipment and storage. Consistent with NUREG 0737, the technical support center is nonsafety-related and is not required to be available after a safe shutdown earthquake.  The size of the TSC complies with the size requirements of NUREG-0696, “Functional Criteria For Emergency Response Facilities.”  The TSC complies with the habitability requirements of NUREG-0737, Supplement 1; “Requirements for Emergency Response Capability” when electrical power is available.  Should habitability be challenged within the TSC due to lack of cooling or a high radiation level resulting from a beyond-design-basis accident, the plant management function of the TSC is transferred to the main control room. |
| (4) The centre shall receive information on the power unit's status during the phases of accident progression and on the radiological conditions at the NPP site and its surroundings. | OR/COM | The AP1000 plant DCD Section 13.3 discusses Emergency Planning and Section 1.2.5 provides the locations of the technical support center, the operations support center and the decontamination facilities. The AP1000 plant DCD Section 9.4 provides a description of the HVAC systems for the MCR/control support area and the annex building. The AP1000 plant DCD Section 18.8 provides the high level requirements for the technical support center and the operations support center. The AP1000 plant DCD Section 7.5 identifies the plant variables that are provided for interface to the emergency planning areas. Communication interfaces among the MCR, the technical support center and the emergency planning centers are discussed in the AP1000 plant DCD Section 13.3.1 |
| (5) The centre shall be equipped with devices and systems for communication with the main and supplementary control rooms, with the authorities of local self-government and the executive power relevant for accident management. The communication systems and devices shall be maintained available, periodically tested and the documentation shall be kept up-to-date. | OR | This is an owner requirement |
| Article 95 | | |
| Prior to the beginning of a power unit commissioning, verification shall be made on the hardware and software, programmes and methodologies which are needed for:  1. functional capability inspection of the SSCs (including those inside the reactor) and their replacement after their design lifetime;  2. functional tests of the systems intended to prove their design characteristics;  3. verification of the signal sequences and actuation of systems and components, including of the emergency power supply;  4. in-service inspection of the base metal and weldings of the structures and pipelines;  5. verification of the metrological characteristics of the measuring channels for compliance with the design requirements. | OR | DCD Chapter 14 describes AP1000 14 Initial Test Program.  AP1000 Commissioning and Startup Test Program is used to demonstrate that the construction of the AP1000 Nuclear Power Plant (NPP) meets the design and safety requirements as specified in the design documentation, Safety Analysis Reports (SAR), and license conditions. The Commissioning and Startup Test Program also serves to ensure that commissioning program activities are performed in a controlled and safe manner and provides the management and administrative controls necessary to direct the preparation, approval, and performance of testing. Existing Specific documents and procedures shall be modified as necessary to reflect project specific details such as the selected Turbine Island (TI) vendor and other site-specific considerations.  The initial plant test program consists of a series of tests categorized as construction and installation, preoperational, and startup tests. These tests are discussed in DCD Section 14.4. This is mainly divided as follows.  - Inactive Testing - includes the complex verification of functional ability of nuclear installation and its final proof performed before the fuel loading into the reactor. There are three phases of Inactive Testing:  - Phase I: Construction Testing  - Phase II: Component Testing  - Phase III: Preoperational Testing, divided in two phases:  - Phase IIIa: Cold functional testing: Includes Main Control Room (MCR) in service, System, SG Hydro, Cold Hydro Test (CHT), Turbine on gear, Diesel unit and Balance of Plant (BOP) support systems  - Phase IIIb: Hot Functional Testing (HFT): Includes Turbine Roll and Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) submittal  - Active Testing – (Phase IV): includes the tests performed from the start with initial fuel loading into the reactor, up to the completion of the Trial Operation: Startup Testing (Initial Fuel Load (IFL), Pre- Critical Tests, Initial Criticality/Low Power Physics Tests (LPPT), Power Accession Tests (PAT), and Performance Tests.  AP1000 plant meets the design related to taking into consideration inspection and maintenance programs. Nonetheless the licensee shall prepare and implement documented programs of maintenance, testing, surveillance, and inspection of SSCs important to safety.  Westinghouse will provide input to the designer for maintenance, testing, surveillance, and inspection developed for AP1000 plant SSCs for the Owner to develop their programs.  For example, the following DCD Sections provide guidance:  • DCD Section 3.2.3 – Inspection requirements  • DCD Section 3.8 – Testing and In-Service Inspection Requirements.  • DCD Section 3.9 – Inservice testing  • DCD Section 4.2.4 – Fuel system testing and inspection plan  • DCD Section 4.6.3 – Testing and verification of the control rod drive system  • DCD Section 5.2.4 – Inservice Inspection and Testing of Class 1 components  • DCD Section 6.6 – Inservice Inspection of Class 2, 3, and MC components  • DCD Section 10.2.3.6 - Turbine Maintenance and Inspection  • DCD Section 10.3.4 – Main Steam Supply Testing and Inspection requirements  • DCD Chapter 13 – Conduct of Operations  • DCD Chapter 16 - Surveillance testing requirements are specified in the plant Technical Specifications  • DCD Section 17.4 – Design Reliability Assurance Program  In the case of Bulgaria some specific permitting might be needed with regard to (5) verification of the metrological characteristics. |

### Section II: Reactor Core Design and Features

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 96 | | |
| (1) The reactor core and associated reactor coolant system, and reactor safety systems shall be designed with appropriate safety margins to ensure that the specified design limits for fuel damage are not exceeded in all operational states and accidents without fuel melting with account taken of:  1. design operational states and their course;  2. thermal, mechanical and irradiation degradation of the core components;  3. physical-chemical interaction of the core materials;  4. limiting values of thermal hydraulic parameters;  5. vibrations and thermal cycles, material fatigue and ageing;  6. impact of coolant impurities and radioactive fission products on the fuel claddings corrosion;  7. irradiation and other impacts that deteriorate the mechanical characteristics of the core materials and fuel cladding integrity. | COM | Reactor core and coolant system is designed with high margins to ensure that design limits for fuel damage are not exceeded with consideration of items 1-7 of this requirement. See DCD sections 4 and 5. |
| (2) The design shall specify the limits for damage of the fuel elements (in terms of amount and degree) and the associated coolant radioactivity according to reference isotopes. | COM | The AP1000 plant DCD [2] Section 4.2 provides the AP1000 plant fuel system design. The plant conditions for design are divided into four categories.  Condition I - normal operation and operational transients  Condition II - events of moderate frequency  Condition III - infrequent incidents  Condition IV - limiting faults  The core design provides adequate margin so that departure from nucleate boiling will not occur with a 95 percent probability and 95 percent confidence basis for all Condition I and II events. The reactor can be brought to a safe state following a Condition III event with only a small fraction of fuel rods damaged. The fraction of fuel rods damaged must be limited to meet the dose guidelines identified in Chapter 15 although sufficient fuel damage might occur to preclude immediate resumption of operation. The reactor can be brought to a safe state and the core kept subcritical with acceptable heat transfer geometry following transients arising from Condition IV events.  Reactor coolant radioactivity is presented in DCD section 11.1. Limiting Condition for Operation is set in Technical Specifications (DCD Chapter 16) 3.4.10 RCS Specific Activity, The limits on RCS specific activity ensure that the doses due to postulated accidents are within the doses reported in Chapter 15, The LCO limits are established to be consistent with a fuel defect level of 0.25 percent and to ensure that plant operation remains within the conditions assumed for shielding and Design Basis Accident (DBA) release analyses. |
| Article 97 | | |
| To ensure safe shutdown of the reactor, to maintain the reactor subcritical and to ensure core cooling, the reactor core and associated core internals located within the RPV shall be designed and installed in such a way as to withstand the static and dynamic loads expected in all operational states, accidents without fuel melting, and external events considered in the design. | COM | Reactor core and internals are designed so that all expected static and dynamic loads are considered, see DCD sections 3.9 and 4. |
| Article 98 | | |
| (1) The reactor core and its components that affect reactivity shall be designed in a way that any reactivity change caused by the control rods as well as reactivity effects shall not lead to fuel damage that exceeds the specified design limits and shall not cause any damage to reactor coolant pressure boundary in all operational states and accidents without fuel melting. | COM | No such reactivity change, or reactivity effect will lead to exceeding of fuel design limits or damage to the reactor coolant boundary. Limits for fuel element damage are specified in DCD section 4 and design basis of reactor coolant boundary in DCD section 5. This is confirmed in deterministic safety analysis (DCD section 15). |
| (2) The design shall prove that in all accidents with fast insertion of positive reactivity, specific energy threshold for fuel damage is not exceeded at any moment of the fuel cycle, and fuel melting is excluded. | COM | Fuel design is presented in DCD section 4. Deterministic safety analyses proves that fuel design limits are not exceeded (DCD section 15). |
| (3) Accidents with fast insertion of positive reactivity, resulting in early or large radioactive releases to the environment shall be practically eliminated. | COM | Practical elimination of events is analyzed in separate report, “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5]. |
| (4) For all accidents without fuel melting, changes in core geometry shall be limited so as to ensure conditions for long-term fuel cooling, insertion of control rods and ensuring core subcriticality for a long period of time. | COM | Reactor core design is presented in DCD section 4. Changes in core geometry is limited so that long-term cooling, insertion of control rods and core subcriticality is ensured. |
| (5) Reactivity feedback, determined by the parameters that affect reactivity, shall be negative in all possible critical states of the reactor, in all operational states and accidents without fuel melting. | COM | Reactivity feedback is discussed in DCD subsection 4.3.1.2 Negative Reactivity Feedbacks (Reactivity Coefficients), in all operating states and accidents without fuel melting. |
| (6) The design shall ensure that after anticipated operational occurrences and accidents without fuel melting, the core shall remain subcritical. | COM | The plant is provided with the means of making and holding the core subcritical under any anticipated conditions and with appropriate margin for contingencies. |
| Article 99 | | |
| (1) The neutron flux distribution shall be stable and shall require minimum intervention for maintaining the shape, level and stability of the neutron flux within defined design limits, for all core states, including after reactor shutdown, during and after core refuelling, and anticipated operational occurrences. | COM | Typical values of the neutron flux distribution and spectrum are presented in DCD Table 4.3-6. Neutron flux distribution is stable, and it is maintained within the design limits for all core states. |
| (2) The design shall provide for adequate means to measure neutron flux distribution so that the design limits in any axial or radial core part are not exceeded during reactor installation power operation. | COM | The in-core instrumentation system includes in-core flux thimbles containing fixed detectors for measurement of the neutron flux distribution within the reactor core, see DCD section 4.2.2. |
| Article 100 | | |
| The reactor core and associated coolant system and safety systems shall be designed to enable adequate inspection and testing throughout the service lifetime of the plant. | COM | Reactor core and coolant system and safety systems are designed to enable adequate inspection and testing. |
| Article 101 | | |
| The characteristics of nuclear fuel, reactor structures and reactor coolant system components (including the coolant clean up system) and considering the operation of the other systems shall exclude accumulation of critical mass in accidents with fuel melting. | COM | Severe accident strategy is presented in DCD section 19, including in- vessel retention of molten core debris. |
| Article 102 | | |
| The fuel elements and assemblies, with account taken of the uncertainties in data, calculations and assumptions in fabrication, shall be designed to withstand irradiation and the reactor core conditions in combination with all degradation processes that can occur in all operational states, such as:  1. differential expansion and deformation;  2. external pressure of the coolant;  3. additional internal pressure in the fuel element due to fission products;  4. irradiation of fuel and other materials in the fuel assembly;  5. variation in pressure and temperatures resulting from variations in power;  6. chemical effects;  7. static and dynamic loads, including flow induced vibrations and mechanical vibrations;  8. variations in heat transfer performance that could be a result of distortions or chemical effects. | COM | Fuel system design basis is presented in DCD section 4.2.1, including items 1-8 presented in this Article. |

### Section III: Reactor Shutdown Systems

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 103 | | |
| (1) The design shall provide for means to control reactivity, that are capable of ensuring reactor shutdown in all operational states and accident conditions, and of maintaining core subcriticality even at the maximum value of the effective neutron multiplication factor. | COM | AP1000 provides adequate means for controlling excess reactivity in the core. The reactivity control of the core depends on control rods, dissolved boron in the coolant, and other poisons. The normal control of the boron concentration is one of the functions of the chemical and volume control system (CVS). The PXS provides the safety-related long-term safe shutdown boration capability.  Release the “black” (Ag-In-Cd) shutdown bank control rods for gravity insertion into the core on power interruption, in response to a reactor trip initiated from either manual or automatic reactor protection system controls, at the required rate to maintain fuel integrity. The worth of the mechanical shim gray rod cluster assemblies (GRCAs) is not credited in safety analyses or the Core Makeup Tank (CMT) sizing or the CMT boron concentration, but the rod worth is credited in Modes 3 (Hot Standby) through 6 (Refueling) when determining shutdown margin supplied from the CVS. |
| (2) The effectiveness, speed of action of reactivity control means, and core criticality margins shall be such that the design limits for fuel damage are not exceeded. | COM | Reactivity control is ensured in AP1000 design. Deterministic safety analyses (DCD section 15) confirms that fuel design limits are not exceeded. |
| Article 104 | | |
| (1) The means for reactivity control shall consist of at least two independent and diverse systems; each one of these systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, considering the single failure principle or human error. | COM | Reactor shutdown by control rod insertion is independent of the normal control functions since the trip breakers interrupt power to the rod mechanism. Two reactivity control systems are provided:  1) Rod cluster control assemblies and gray rod assemblies.  2) chemical shim (boric acid)  For slowly evolving events, AP1000 plant uses rod cluster control assemblies and chemical shim as the two diverse reactivity control systems. For fast transients, AP1000 plant provides several additional features to supplement the chemical shim control systems. These diverse features include a diverse actuation system (DAS) which provides a different way of cutting off power to the rod cluster control assemblies (in case there is a common cause failure of the reactor trip breakers).  Another diverse feature is the ability of the AP1000 plant to “ride out” an anticipated transient event without insertion of rod cluster control assemblies using the core characteristics (such as a negative moderator coefficient) to reduce the reactor power. The DAS also supports “ride out” by actuating a turbine trip and start of the passive residual heat removal heat exchanger.  The rod cluster control assemblies and gray cluster control assemblies are inserted into the core by the force of gravity. See the AP1000 plant DCD [2] Section 3.1 GDC 26. During operation, the shutdown rod banks are fully withdrawn. The control rod system automatically maintains a programmed average reactor temperature compensating for reactivity effects associated with scheduled and transient load changes. See the AP1000 plant DCD [2] Section 4.3 for additional information.  The shutdown and control rod banks are designed to provide reactivity margin to shut down the reactor during normal operating conditions and during AOOs, without exceeding specified fuel design limits.  The safety analyses assume the most restrictive time in the core operating cycle and that the most reactive control rod cluster assembly is in the fully withdrawn position. See the AP1000 plant DCD [2] Chapter 15 for summaries of the analyses, assumptions, and results. The passive safety systems provide the required boration to establish and maintain safe shutdown condition for the reactor core. See the AP1000 plant DCD [2] Section 6.3 and the AP1000 plant DCD [2] Section 3.1 GDC 26 for additional information.  The PMS provides the safety functions necessary to shut down the plant, and to maintain the plant in a safe shutdown condition. The PMS controls safety components in the plant that may be operated from the MCR or remote shutdown workstation.  The DAS provides a diverse means of initiating the reactor trip and emergency safety features. The PMS is designed to prevent common mode failures; however, in the low-probability case of a common mode failure, the DAS provides diverse protection.  When fuel assemblies are in the pressure vessel and the vessel head is not in place, keff will be maintained at or below 0.95 with control rods and soluble boron. Further, the fuel will be maintained sufficiently subcritical that removal of the rod cluster control assemblies will not result in criticality. |
| (2) The systems shall be adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality during the reactor shutdown, or during core refuelling operations or other routine or non-routine operations in the reactor shutdown state. | COM | Reactivity control systems are adequate to prevent any foreseeable increase in reactivity leading to unintentional criticality. |
| (3) The system design shall consider possible internal or external system failures that could render part of reactivity control means inoperative, or that could result in a common cause failure of the whole system. | COM | As presented in DCD section 4.6.2, rod control systems have been analyzed in detailed reliability studies. These studies include fault tree analysis and failure mode and effects analyses.  These studies, as described in the AP1000 plant DCD [2] Chapter 15, show that the AP1000 plant design has sufficient shutdown margin even assuming that the highest worth rod cluster control assembly fails to insert.  The protection and reactivity control systems have an extremely high probability of performing their required safety functions in the event of AOOs. High quality equipment, diversity, and redundancy, support this probability. Loss of power to the protection system results in a reactor trip. Defense in depth is designed into the AP1000 plant to reduce challenges to the protection and reactivity control systems. See the AP1000 plant DCD [2] Section 3.1 GDC 29.  Sufficient redundancy and independence are designed into the protection systems so that no single failure or removal from service of any component or channel of a system results in loss of the protection function. Functional diversity and location diversity are designed into the system. The diverse reactivity control system is chemical shim which for the purpose of this discussion includes the core makeup tanks. The reliability of these tanks is greater than 10-3 /demand. The DAS reliability is conservatively assumed to be 10-2 / demand (auto). |
| Article 105 | | |
| (1) At least one of the systems shall perform reactor emergency shutdown functions and shall maintain core subcritical with sufficient margin, taking into account failure to activate the most effective control rod and maximum value of the effective neutron multiplication factor. | COM | Reactivity control is ensured by control rods. Sufficient margins with the consideration of failure of the most effective control rod and maximum value of the effective neutron multiplication factor are considered. This is confirmed in deterministic safety analysis (DCD section 15). |
| (2) In case the effectiveness of the emergency shutdown system is not sufficient to maintain the core subcritical for a long time, provisions shall be made for automatic actuation of another reactor shutdown system with adequate effectiveness to maintain the core subcritical, considering possible reactivity release. | COM | As indicated in DCD section 15, there are three postulated events that assume credit for reactivity control systems, other than a reactor trip to render the plant subcritical. These events are the steam-line break, feedwater line break, and small break loss of coolant accident. The reactivity control systems in these accidents are the reactor trip system and the passive core cooling system (PXS). |
| (3) The reactor emergency shutdown system shall have at least two independent groups of rods. The control rods shall be actuated at any intermediate or operating position. | COM | Control rod patterns and their design basis are presented in DCD section 4.3.2.5. |
| (4) Any possibility for positive reactivity insertion by means of reactivity control shall be excluded by technical means if the emergency shutdown system rods have not been inserted in operating position. | COM | Technical means are provided against positive reactivity insertion. Neutron flux monitoring actuates reactor trip when positive reactivity insertion could occur. |
| Article 106 | | |
| (1) All emergency shutdown system rods shall have intermediate position indicators, end position annunciators and limit switches (end breakers), actuated where practicable directly by the control rod. The other reactivity control means shall be equipped with position indicators as a minimum. | COM | Control rod position monitoring is presented in DCD section 7.7.1.3, including digital rod position indication and demand position system. |
| (2) The design shall determine tests required to confirm the operability of the reactivity control means, envisaged for each operational state of the NPP. | COM | Necessary tests are provided to confirm the operability of the reactivity control including the verification that the trip time achieved by the CRDMs meets the design requirements. |

### Section IV: Instrumentation and Control Systems

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 107 | | |
| (1) The control systems shall measure the values of key parameters that could impact the chain fission reaction, the nuclear fuel integrity in the core and in the spent fuel pools, the reactor coolant boundary system and the containment in all operational states and accident conditions. | COM | DCD section 7 presents control systems, including the AP1000 plant PLS and the PMS, and other systems, and its design basis, including monitoring of the key parameters. |
| (2) The instrumentation and recording equipment shall ensure sufficient information for monitoring the status of essential equipment and the course of accidents, for determining the amounts and locations of releases of radioactive substances in the environment, and for post-accident analysis. | COM | DCD section 7 presents control systems and its design basis, including monitoring of the key parameters.  The PMS is the aggregate of electrical and mechanical equipment which senses generating station conditions and generates the signals to actuate reactor trip and engineered safety features functions, and which provides the equipment necessary to monitor plant safety functions during and following designated events as required by Regulatory Guide 1.97. See AP1000 plant DCD [2] Sections 7.1.2 and 7.5. |
| (3) The changes in normal operation conditions which may affect safety, shall be accompanied by audible and visible indication in the main control room. | COM | As presented in DCD section 7.1.1, the main control room is implemented as a set of compact operator consoles featuring color graphic displays and soft control input devices. The graphics are supported by a set of graphics workstations that take their input from the real-time data network. An advanced alarm system, implemented in a similar technology, is also provided. |
| (4) The control systems shall be adequate for measuring the NPP parameters and shall be qualified for environmental conditions in normal operation, anticipated operational occurrences and accident conditions. | COM | Control systems are adequate to measure NPP parameters, and they are qualified for environmental conditions in normal operation, AOOs and accidents. |
| Article 108 | | |
| (1) The normal operation control systems shall reliably maintain and control variations of process parameters within the operational limits. | COM | The plant control system is a nonsafety-related system that provides control and coordination of the plant during startup, ascent to power, power operation, and shutdown conditions, see DCD section 7.1.3. |
| (2) Control signals of technological systems and components important to safety, formed by the control systems or by the MCR remote control switches, shall be automatically recorded. | COM | Principles for recording are presented in DCD section 7.5. Recording is provided always for category I and as required for categories II and III. In order to provide operators with a comprehensive picture of historical events, the PLS provides sequence of events recording for PMS signals. |
| Article 109 | | |
| (1) The control safety systems shall detect indications of potential accidents and shall automatically actuate the safety systems necessary for achieving and maintaining safe plant conditions. | COM | DCD section 7 presents control systems and its design basis, including monitoring of key parameters and automatic actuation of safety systems with Protection and Safety Monitoring System (PMS). |
| (2) The control safety systems shall be designed so that:  1. a single failure does not result in loss of control function;  2. unavailability of any component or train does not result in loss of the required minimum redundancy;  3. they shall be capable of overriding unsafe impacts of the control systems for normal operation;  4. they shall prevent operator actions that could compromise the efficiency of the protection system in operational states and in accident conditions, but shall not counteract correct operator actions in accident conditions;  5. in the event of a failure of a control safety system they shall achieve safe plant conditions by implementing the fail-safe principle;  6. they shall actuate the safety systems so that operator action is not necessary within a certain period of time from the onset of anticipated operational occurrences or accident conditions;  7. they shall make relevant information available to the operator for monitoring the effects of the automatic actions;  8. they shall ensure continuous automatic diagnostics of the systems operability and diagnostics of the technological components whose failures are initiating events for accidents. | COM | DCD section 7 presents control safety systems and its design basis.   1. Single failures are considered in the control functions. 2. The unavailability of any component/train does not result in the loss of minimum redundancy. 3. Prioritizing of safety functions is provided. 4. Operator actions, which could endanger nuclear safety are prevented by control systems, but correct actions are allowed. Design includes interlocks and permissives. 5. Fail-safe principle is applied in the design. 6. The safety‐related passive systems are designed to operate for at least 72 hours without any ac power. In fact, the passive systems are designed to not only bring the plant to a controlled state following a station blackout, but to actually automatically, and without operator action, to bring and maintain the plant to a safe shutdown condition for at least 72 hours.   In general where operator actions are taken, the AP1000 design is based on previous experience and the guidance of ANSI 58.8‐1984 a 30-minute rule is applied so that operator actions are not needed at least in 30 minutes after the AOO or accident.   1. Relevant instrumentation for monitoring the plant status is provided. 2. Automatic and continuous diagnostics of the system operability is provided |
| Article 110 | | |
| (1) The instrumentation and control systems for SSCs important to safety shall be designed with high functional reliability and possibility for periodic testing conformable to the safety function to be performed. | COM | DCD section 7 presents control safety systems and its design basis.  High reliability is ensured for instrumentation and control systems and possibility for periodic testing is provided. |
| (2) Principles such as functional diversity and diversity in component design, independence and redundancy shall be used in the design to the extent practicable to prevent the loss of safety functions. | COM | DCD section 7 presents control safety systems and its design basis.  Nuclear safety design principles, such as diversity, independency and redundancy are applied in the I&C design. |
| (3) Periodic testing shall determine the functionality of sensors, input signals, logics, technical controls and technical and computer means of recording. | COM | DCD section 7 presents control safety systems and its design basis.  Periodic testing is provided for I&C design. |
| (4) When a safety system has to be taken out of service for periodic testing during power operation, provision shall be made in the design for the clear indication of any system bypass that is necessary for the duration of the testing or maintenance activities. | COM | Necessary indications and system bypass features are provided for testing and maintenance purposes, see DCD section 7.  The I&C equipment performing reactor trip and ESF actuation functions, their related sensors, and the reactor trip switchgear are, for the most part, four-way redundant. This redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a two-out-of-three logic from a two-out-of-four logic. |
| Article 111 | | |
| (1) When designing computer based instrumentation and control systems for SSCs important to safety, appropriate standards and practices shall be identified and implemented to ensure high quality of development and testing of computer hardware and software throughout the service life of the systems, in particular when developing the software. | COM | The instrumentation and control systems are designed in accordance with guidance provided in applicable portions of the standards presented in DCD section 7.1.4.2. Computer hardware and software testing is provided. Special attention is provided when software is developed from HFE point of view, see DCD section 18.8.1.10. |
| (2) The entire development process, including control, testing and introducing of design changes, shall be systematically documented so as to allow traceability and reviewing. | COM | Development process, including control, testing and possible design changes are systematically document. |
| (3) Equipment reliability assessment shall be undertaken by experts who are independent of the designer and the supplier. Where safety functions are essential for achieving and maintaining safe plant conditions, and the necessary high reliability of the hardware and software cannot be demonstrated with a high level of confidence, diverse means of ensuring fulfilment of the safety functions shall be provided. | COM  NAS | The diversity principle is applied in the AP1000 I&C design to ensure high reliability, see DCD section 7 and e.g., description of Diverse Actuation System (DAS) in DCD section 7.7.1.11.  Requirement needs to be considered in the design process to ensure that independent experts of the design and supplier are used for equipment reliability assessment. |
| (4) Common cause failures deriving from software shall be taken into consideration for the assessment of the safety functions performance. | COM | Software common cause failures are considered in the I&C architecture so that there are diverse means for safety function performance, see DCD section 7 and description of Diverse Actuation System (DAS) in DCD section 7.7.1.11. |
| (5) Protection shall be provided against accidental disruption of, or deliberate interference with system operation. | COM | Design features are provided to protect the NPP against accidental disruption and deliberate interference. |
| Article 112 | | |
| (1) Interference between control safety systems and control systems for normal operation shall be prevented by means of separation, by avoiding common connections or by functional independence. | COM | Functional isolation is applied between normal operation and safety systems to prevent interference between normal operation and safety I&C, see DCD section 7. |
| (2) When common signals are used, adequate electrical separation (decoupling) shall be ensured and signals shall be classified as part of the control safety system. | COM | As presented in DCD section 7.1.2.10, isolation devices are used to maintain the electrical independence of divisions, and to prevent interaction between nonsafety-related systems and the safety-related system. |
| (3) Instrumentation and control systems for the hardware and software intended for multiple failure protection and for containment protection in accidents with fuel melting, shall be separated and independent from the other instrumentation and control systems as far as practicable. Active system components shall be redundant. | COM  CWO | I&C architecture is presented in DCD chapter 7.1. Separation and redundancy principle is applied in AP1000 I&C design. Design includes Protection and Safety Monitoring System (PMS) for safety-related functions necessary to achieve and maintain the plant in safe shutdown conditions. In addition, I&C architecture includes Diverse Actuation System (DAS) that provides an alternate means for reactor trip and selected safety functions, in case of multiple errors leading to unavailability of PMS.  There is no separate I&C system designed for containment protection in accidents with fuel melting. PMS and DAS are used for accidents in fuel melting, which are diverse from each other. Due to the robust design of AP1000 and based on the results from deterministic and probabilistic safety assessments (DCD section 15 and 19), it is considered that there is sufficient independency available for accident management. |
| Article 113 | | |
| (1) The MCR shall provide the opportunity to operate safely the nuclear power plant in all operational states, both automatically or manually; it shall be possible to take measures in the MCR to maintain the plant in a safe state or to bring it back to a safe state after anticipated operational occurrences and accident conditions. | COM | A main control room is provided that can control the plant during normal and anticipated transients and design basis accidents. The main control room includes indications and controls capable of monitoring and controlling the plant safety systems as well as the nonsafety-related control systems. |
| (2) The layout of instrumentation and control devices and the way of presenting the information shall be such that the operating crew at the MCR are able to clearly and quickly identify the plant status and behaviour, adherence to the operational limits and conditions, identification and diagnosis of the safety system automatic actuation and functioning, and accident management systems functioning. | COM | Human factors engineering principles (see DCD section 18) are applied in the layout of I&C and in the way of presenting information to ensure that operating personnel can clearly and quickly identify the plant status and behavior. |
| (3) The design shall identify those events, both internal and external to the MCR, that could directly challenge its continued operation, and shall provide for reasonably practicable measures to contain the consequences of such events. | COM | Those events are identified, which can affect the continued operation of MCR. Technical design features are considered in control room design to ensure continued operation. Remote shutdown station is included to the design to ensure plant safe control and monitoring, if MCR is unavailable. |
| (4) The MCR operating personnel shall be protected by provision of barriers against high radiation levels resulting from accident conditions, releases of radioactive substances, fire, or explosive or toxic substances. | COM | Habitability systems are provided in the design to ensure that operating personnel is protected against radiation and other dangerous gases, see DCD section 6.4.  The main control room emergency habitability system (VES) provides a supply of breathable air for the main control room (MCR) occupants and maintains the MCR at a positive pressure with respect to the surrounding areas whenever ac power is not available to operate the nuclear island nonradioactive ventilation system (VBS) or high radioactivity is detected in the MCR air supply.  The temperature and pressure in the MCR are maintained so that the combination of initial MCR environment conditions, minimized MCR equipment heat sources, MCR isolation, VES-supplied air, VES filtration, and MCR in leakage limitations adequately support the allowable number of MCR inhabitants for 72 hours after an accident. After 72 hours, the licensing and design basis is that VBS functionality is restored and that VBS fully supports MCR habitability.  VES is a passive safety system, It passively provides air form compressed air tanks, maintaining MCR overpressure and air filtration. MCR heat removal counts on passive heat sinks (structures and equipment inside the MCR envelop that absorb heat).  During Normal Operation Nuclear Island Nonradioactive Ventilation System (VBS) will provide the HVAC and control room habitability, supplying the MCR envelope. It will also serve other non-radioactive areas in the nuclear island that include Class 1E and non-1E electrical equipment rooms, remote shutdown workstation HVAC equipment rooms in the Auxiliary Building; Control Support Area/Technical Support Center (CSA/TSC) area in the Annex Building; and Passive Containment Cooling System (PCS) valve room in the Shield Building.  VBS shall:  • Provide isolation of the MCR envelope from the surrounding areas and outside environment during and following a design basis accident.  • Provide radiological monitoring of MCR supply air airborne process streams and initiation signals to the Protection and Safety Monitoring System (PMS) for actuation of the Main Control Room Emergency Habitability System (VES).  • After 72 hours after and accidental condition this system functionality is to be restored and provide MCR Habitability.  • Provide protection of MCR and/or CSA areas from infiltration of smoke from an external source.  • Provide smoke removal capability for the MCR envelope, CSA area and Class 1E electrical equipment rooms from an internal source. |
| Article 114 | | |
| (1) The supplementary control room (SCR) shall enable the following functions:  1. control of the safety systems;  2. rendering and maintaining the reactor subcritical;  3. heat removal from the reactor coolant system and from the spent fuel pool;  4. control of the status of the reactor installation and of the spent fuel pool. | COM | Remote shutdown workstation is included to the design to ensure plant safe control and monitoring, if MCR is unavailable, enabling the performance of the safety function 1-4 presented in this requirement, see DCD section 7.4.3.  The Remote Shutdown Workstation (RSW) contains the indications and controls that allow an operator to achieve and maintain safe shutdown of the plant following an event when the MCR is unavailable. The RSW is not normally powered and requires control to be manually transferred from MCR if there is an event that requires evacuation of the MRC.  Additional non-safety-related indications and controls are provided. As with the MCR, the RSW requires no ac power sources for its operation.  Additionally, a secondary diverse actuation is located in a diverse spatially separated location to actuate key safety functions such as ADS Stage 4 actuation, IRWST injection and containment recirculation actuation. The secondary DAS panel is powered by an independent local battery. The secondary DAS panel is located sufficiently far from the Main Control Room (MCR) and Remote Shutdown Work Station), its location has been selected as to provide additional protection so that it is very unlikely that it could be affected by internal events such as fire, internal flooding, or external events such as flooding (thus providing additional protection from these events). |
| (2) The SCR shall be physically, electrically and functionally separate from the MCR. Any possibility of parallel actuation of control components from the MCR and the SCR, shall be eliminated by technical means. Appropriate measures shall be taken to eliminate any possibility for failure of the control circuits of both MCR and SCR due to a common cause, in postulated initiating events. | COM | Remote shutdown workstation is physically, electrically, and functionally separated from the MCR and there is no possibility for parallel operation, see DCD section 7.4.3. |
| (3) The SCR shall be designed to protect the personnel in all conditions resulting from internal and external events and in accident conditions. | CWO | The remote shutdown workstation is provided for use only following an evacuation of the main control room due to fire. No actions are anticipated from the remote shutdown workstation during normal, routine shutdown, refueling, or maintenance operations. |

### Section V: Reactor Coolant System

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 115 | | |
| (1) The reactor coolant system and its associated safety systems shall be designed with sufficient margins to ensure that design limits of the reactor coolant pressure boundary are not exceeded in all operational states. | COM | Reactor coolant system and associated safety systems (see DCD section 5) are designed with sufficient safety margins to ensure that design limits for pressure boundary are not exceeded.  The design transients used in the design and fatigue analysis of American Society of Mechanical Engineers (ASME) Code Class 1 and Class CS components, supports, and reactor internals are provided in subsection 3.9.1. The loading conditions, loading combinations, evaluation methods, and stress limits for design and service conditions for components, core support structures, and component supports are discussed in DCD subsection 3.9.3.  The AP1000 RCPB is consistent with that of 10 CFR 50.2. |
| (2) Provisions shall be made in the design for pressure relief devices to protect the pressure boundary of the reactor coolant systems against overpressure and to prevent unacceptable releases of radioactive substances to the environment in all operational states and accidents without fuel melting. | COM | Pressure relief devices are provided to protect against overpressure and radioactive releases in all operating states and accidents without fuel melting, see DCD section 5.2.2.  Overpressure Protection for RCS and steam system overpressure protection during power operation are provided by the pressurizer safety valves and the SG safety valves, in conjunction with the action of the reactor protection system. Combinations of these systems provide compliance with the  overpressure protection requirements of the ASME Boiler and Pressure Vessel (B&PV) Code, Section III, Paragraphs NB-7300 and NC-7300, for pressurized water reactor (PWR) systems.  Low temperature overpressure protection is provided by two relief valves in the suction line of the normal RNS. |
| (3) The design of pipework connected to the pressure boundary of the reactor coolant systems shall provide for isolation devices to limit any leak of primary coolant and to prevent the loss of coolant through interfacing systems. | COM | AP1000 reactor coolant pressure boundary is consistent with that of 10 CFR 50.2.  Section 50.2 of 10 CFR 50 defines the reactor coolant pressure boundary as vessels, piping, pumps, and valves that are part of the reactor coolant system (RCS), or that are connected to the reactor coolant system up to and including the following:  • The outermost containment isolation valve in system piping that penetrates the containment  • The second of two valves closed during normal operation in system piping that does not penetrate containment  • The reactor coolant system overpressure protection valves.  The term reactor coolant system, as used in this section, is defined in Section 5.1 of the DCD.  Isolation devices are provided to ensure any coolant loss through interfacing systems. As presented in DCD section 5.4.3.2.1, the boundary of the reactor coolant system includes the second of two isolation or shut off valves and the piping between those valves. Also, a single ASME Code safety valve may also represent the boundary of the reactor coolant system. |
| Article 116 | | |
| (1) Components, pipelines and supporting structures of the reactor coolant system shall withstand all static and dynamic loads and temperature effects to any of their component in all operational states and accidents without fuel melting. | COM | Reactor coolant system components (see DCD section 5) are designed to ensure that all static and dynamic loads and temperature effects are considered in all operating states and accidents without fuel melting, see DCD section 3.9 and DCD section 5. |
| (2) Materials to be used for fabrication of the components of the reactor coolant system shall be selected so as to minimise their activation and the probability of crack propagation and neutron embrittlement, with account taken of the expected degradation of their characteristics at the end of their lifetime under the effects of erosion, creep, fatigue and chemical impacts. | COM | Material selection requires a balance between structural considerations (such as maintaining pressure-vessel integrity), cost, and minimizing the radioactivity in the primary circuit so far as is reasonably practicable. Thus components materials are selected so that they minimize their activation, probability of crack propagation and neutron embrittlement, see DCD section 5.2. Material specifications are presented in DCD table 5.2-1.  As a general principal, Westinghouse chooses to use only proven materials in the primary circuit, and takes effort to minimize the corrosion of these materials. As part of the selection process, Westinghouse engineers considered both previous records of service for a given material, along with any recent published data or research.  Materials in the primary circuit can be divided into two groups: “In-Core materials” and “Out-of-Core materials.” The first group consists of materials used in the reactor and exposed to irradiation at their primary location. The second group comprises materials used within the primary circuit and steam generators, outside the reactor core. Material from out-of-core locations can only become activated in the form of corrosion/wear products removed from their primary location and deposited in the core (crud) where they can become activated by neutron irradiation. This crud can in-turn become mobile and re-deposit elsewhere in the primary circuit, creating the out-of-core radiation fields which are of concern, resulting in Operational Radiation Exposure.  Especial attention is given to reduce the Co-60 isotope production. Cobalt-60 is a result of a 59Co nucleus undergoing neutron capture. 60Co decays into 60Ni with a beta decay followed by two high-energy gamma emissions. The quantities of cobalt entering the primary coolant are relatively low compared to the amount of nickel species entering the core, but the probability of activation by neutrons is 170 times that of activating 58Ni. The relatively long half-life and high dose rates mean that 60Co is considered the most hazardous of the activated corrosion products. Main input of 59Co into the primary-circuit coolant comes from impurities in nickel (used in the nickel-based alloys and stainless steels) and high-cobalt alloys such as Stellite.  Thus the following is performed:  - Reduction in the quantities of high-cobalt alloys present in the primary circuit by reducing the number of components that would traditionally be made of high-cobalt alloys and, where applicable, producing components from low-cobalt alloys; and  - Control of manufacturing specifications of materials to control cobalt content of alloys (for example, reducing the acceptable limit of trace cobalt content in alloys). |
| (3) The design shall provide for at least three independent diverse systems for coolant boundary system early leak detection. | COM | DCD section 5.2.5 presents principles for detection of leakage through reactor coolant pressure boundary. Diverse measurement methods including level, flow, and radioactivity measurements are used for leak detection. |
| Article 117 | | |
| The reactor pressure vessel and pressure tubes shall be designed and manufactured to ensure the highest quality with respect to material selection, design standards, capability of inspection and fabrication. | COM | Highest quality is applied to equipment class A, which applies to the reactor coolant system pressure boundary, see DCD section 3.2. This class has the highest integrity, and the lowest probability of leakage. |
| Article 118 | | |
| The design of the components contained inside the reactor coolant pressure boundary shall be designed such as to minimise the likelihood of failure and associated consequential failure and damage to other items of the primary coolant system in all operational states and in accidents without fuel melting. | COM | Reactor coolant pressure boundary materials and fabrication techniques are such that there is a low probability of gross rupture or significant leakage. The AP1000 reactor coolant system design incorporates revised pipe-break criteria (leak-before-break) to reduce or eliminate the need to consider the dynamic effects of pipe breaks. The configuration and materials of the reactor coolant system have been selected such that the pipe stresses meet the leak-before-break criteria. See DCD section 3.6.3 for additional information.  Highest quality is applied to equipment class A, which applies to the reactor coolant system pressure boundary, see DCD section 3.2. This class has the highest integrity, and the lowest probability of leakage. |
| Article 119 | | |
| (1) The components of the reactor coolant pressure boundary shall be designed, manufactured and situated in a way allowing periodical inspections and tests to be carried out throughout the service lifetime of the plant. | COM | DCD subsection 5.2.4 Inservice Inspection and Testing of Class 1 Components, describes this topic.  ASME Code Class 1 components are designed so that access is provided in the installed condition for visual, surface, and volumetric examinations specified by the ASME Code Section XI (1998 Edition) and mandatory appendices. Design provisions, in accordance with Section XI, Article IWA-1500, are incorporated in the design processes for Class 1 components. Arrangement and Inspectability of components is discussed in DCD subsection 5.2.4.2  As presented in DCD table 3.2-1, inspection and testing requirements are applicable to the equipment class A components, which includes reactor coolant system pressure boundary. Hence components are built to ASME Code, Section III are inspected to ASME Code, Section XI requirements. Class A, B, and C structures, systems, and components that are required to function to mitigate design base accidents have some testing requirements included in the plant technical specifications. In addition to the requirements in the technical specifications, testing and maintenance requirements are included in an administratively controlled reliability assurance plan.  Reactor Vessell Inservice Inspection/Inservice Testing is described in DCP subsection 5.3.1.4  The RCP piping and components construction is subject to a quality assurance program. The pressure boundary components meet requirements established by the ASME Code and ASME NQA 1. The testing in the quality assurance program is outlined in DCD the tables of DCD Subsection 5.4 (e.g., Tables 5.4-8, 5.4-6, 5.4-12) |
| (2) The implementation of a material surveillance programme for the reactor coolant pressure boundary shall ensure control of the effects of irradiation, stress corrosion cracking, embrittlement, and ageing of structural materials, particularly in locations of high irradiation, and other factors. | COM | For the reactor vessel, a material surveillance program is provided. see DCD section 5.3.2.6. The material properties surveillance program includes conventional tensile and impact tests and fracture mechanics specimens. The observed shifts in the nil-ductility transition reference temperature of the core region materials with irradiation is used to confirm the allowable limits calculated for operational transients. |
| Article 120 | | |
| The design shall provide for means for controlling the inventory, temperature and pressure of the reactor coolant which have sufficient capacity to ensure that the specified design limits are not exceeded in any operational state, with due account taken of volumetric changes and leakage. | COM | Reactor coolant system design basis is provided in DCD section 5.1.1. Control of inventory, temperature and pressure of the reactor coolant is considered in the design so that design limits are not exceeded.  Control and Instrumentation Systems of the AP1000 described in the DCD Section 7.7 regulate the operating conditions in the plant automatically in response to changing plant conditions and changes in plant load demand. These operating conditions include the following: Reactor Coolant System Temperature, Nuclear Power Distribution, Reactor Coolant System Pressure, Pressurizer Water Level, etc. |
| Article 121 | | |
| (1) The design shall provide for systems to cleanup the reactor coolant from radioactive substances, including activated corrosion products and fission products. | COM | Reactor coolant purification is provided with Chemical and Volume Control System, see DCD section 9.3.6. |
| (2) The capacity of the necessary systems under para. 1 shall be based on the fuel design limits on permissible leakage with a conservative margin to ensure that the coolant activity is as low as reasonably practicable. | COM | As presented in DCD section, 9.3.6.1.2.1, the chemical and volume control system is designed to maintain the reactor coolant system activity level at less than the technical specification limit for normal operations, with design basis fuel defects. The technical specifications allow these limits to be exceeded for a specified duration, see DCD section 16 Technical Specification 3.4.10 RCS Specific Activity. |

### Section VI: System for Core Cooling and Heat Transfer to an Ultimate Heat Sink

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 122 | | |
| The NPP design shall provide for the following to perform the main safety function of "heat transfer from the core to an ultimate heat sink" after scheduled shutting down of the reactor, during and after anticipated operational occurrences and in accident conditions:  1. reactor core residual heat removal (transfer) systems;  2. emergency core cooling systems;  3. systems for heat transfer (removal) to an ultimate heat sink. | COM | Reactor coolant shutdown heat removal is normally provided with normal residual heat removal system, see DCD section 5.4.7. System is not a safety-related system, and it is not needed in accident conditions.  Reactor core residual heat removal system, emergency core cooling systems and systems for heat transfer to an ultimate heat sink are presented in DCD section 6.  Unique to the AP1000 plant design is the use of the steel containment vessel with cooling from the Passive Containment Cooling System (PCS). This provides a path for the removal of decay heat from the containment atmosphere to the environment as the safety-related ultimate heat sink. The safety-related passive systems can maintain Safe Shutdown Conditions for a period of 72 hours -- without operator action and without onsite and offsite AC power sources including the decay heat transmission to the ultimate heat sink (the environment air) though the passive heat removal heat exchanger (PHRHX) to the in containment refueling water storage tank (IRWST), the water will then evaporate and will return after being condensed in the metallic surface of the containment with the help of the passive containment cooling system (PCS) this process can be seen in reference [11].  See also section 1.4.6 Robust Protection of this report |
| Article 123 | | |
| The systems for reactor core residual heat removal in shutdown state of the reactor plant shall be designed with sufficient capacity to ensure the design limits are not exceeded for the fuel, reactor coolant boundary system and the structures important to safety. | COM | Heat removal in shutdown state is ensured with sufficient capacity.  Reactor coolant shutdown heat removal is normally provided with normal residual heat removal system, see DCD section 5.4.7. The system is not a safety-related system and it is not needed in accident conditions.  Reactor core residual heat removal system is presented in DCD section 6. Deterministic safety analyses (DCD section 15) confirms that design limits are not exceeded. |
| Article 124 | | |
| (1) The emergency core cooling systems shall ensure restoration and maintaining of the nuclear fuel cooling in accident conditions, including when the coolant boundary system integrity is breached. In order to achieve reliable safety function performance the systems design shall consider loss of off-site power and single failure, and ensure sufficient redundancy, diversity and independence. | COM | Passive core cooling system is presented in DCD section 6.3. The AP1000 design provides for safety-related passive reactor coolant makeup. Core makeup tanks accommodate small leaks when the normal makeup system is unavailable and provide safety injection for small-break loss of coolant accidents. Accumulators provide the high makeup flow required for a large loss of coolant accident and initiate injection when the reactor coolant system pressure is below the static accumulator pressure during a small-break loss of coolant accident.  Emergency core cooling system design considers single failure criteria, loss-of offsite power, diversity, and independency. The effectiveness of the passive core cooling system is confirmed with deterministic safety analysis, see DCD section 15. |
| (2) The effectiveness of the emergency core cooling systems together with the envisaged technical means for leak detection of the reactor coolant system, the reactor inherent safety features, and the isolation capabilities, shall be sufficient to fulfil the following requirements:  1. meet the criteria for fuel cladding leak-tightness and fuel integrity;  2. maintain within acceptable limits possible chemical reactions of interaction of the substances in the core;  3. possible changes of the internal core geometry shall allow for moving of the control rods and sufficient coolant flow to maintain adequate core cooling;  4. provisions shall be made to ensure conditions for the required time of core cooling, including sufficient coolant inventory. | COM | Passive core cooling system is presented in DCD section 6.3. The AP1000 design provides for safety-related passive reactor coolant makeup. Core makeup tanks accommodate small leaks when the normal makeup system is unavailable and provide safety injection for small-break loss of coolant accidents. Accumulators provide the high makeup flow required for a large loss of coolant accident and initiate injection when the reactor coolant system pressure is below the static accumulator pressure during a small-break loss of coolant accident.  The effectiveness of the passive core cooling system with the consideration of items 1-4 in this requirement are included in the design. The design basis are confirmed with deterministic safety analysis, see DCD section 15. |
| (3) The actuation and operation of the emergency core cooling systems shall not lead to impairment or loss of functions of other systems. Therefore, measures shall be designed to prevent:  1. the possibility for reactor criticality;  2. violation of the protection criteria of reactor coolant pressure boundary, specified in the design limits. | COM | Actuation and operation of the passive core cooling system does not lead to impairment of other systems. Passive core cooling system as a part of mitigation of accidents and as an initiator (e.g., inadvertent operation of the CMT) is extensively analyzed in deterministic safety analyses, see DCD section 15. |
| (4) The design shall provide for opportunities for long-term heat removal in accidents with core melting. | COM | Long-term heat removal in accidents with core melting is considered within severe accident strategy, see DCD section 19.34. |
| 5) The emergency core cooling system design shall permit periodical inspections of the components and periodical testing of the systems to confirm:  1. the integrity of the structure and the tightness of system components;  2. the functional capability and the operational characteristics of active system components;  3. the functional capability of the system as a whole under specified operational states. | COM | The AP1000 passive core cooling system is designed to permit the periodic inspection and testing of the appropriate system components. The testing capabilities of the system including in-service testing and inspection to confirm the structural and leaktight integrity of various components, technical specification operability and performance of the active system components, and additional in-service testing to confirm the overall operability of the system, see DCD section 6.3.6. |
| Article 125 | | |
| (1) The systems and means for transfer of heat from the reactor core and SSCs important to safety to an ultimate heat sink shall perform their function in all operational states and accident conditions with a very high degree of reliability. The reliability to perform this function shall be ensured by simultaneously applying the principles of redundancy, diversity, physical separation, functional separation with allowance made for loss of the main ultimate heat sink or the interface to it. | COM | Passive core cooling system (DCD section 6.3) and Passive Containment Cooling System (6.2.2) provides heat removal with a very high degree of reliability. Systems are designed with the considerations of nuclear safety principles, such as redundancy, diversity, separation, and autonomy. High reliability is confirmed with probabilistic safety assessment, see DCD section 19.  See also section 1.4.2 to 1.4.5 of this Report. |
| (2) The main and alternative systems and means for heat transfer shall be capable of performing their function entirely independent from one another in accident conditions. | COM | AP1000 design includes several ways for heat removal, including safety-related functions and nonsafety functions.  See sections 1.4.2 to 1.4.5 of this Report. |
| (3) The choice of main and alternative ultimate heat sink and the design of heat transfer systems shall be made with account taken of the site-specific natural phenomena and man-induced events with the purpose of ensuring the performance of the function under conditions of extreme external events. | COM  COM-B | Passive containment cooling system provides reliable safety-related ultimate heat sink to the atmosphere (see DCD section 6.2.2).  Design includes consideration of external hazards and man-induced events. However, site-specific hazards may require further considerations. This needs to take into account the recommendations in [9] and [10] these include site seismic and temperature characteristic. AP1000 maximum and minimum external design temperatures are 46,1°C (115°F) and -40°C (-40°F) respectively, AP1000 taking into account the passive safety features of the design, will not suffer a complete loss of its safety functions but a progressive deterioration of these passive safety systems performance (e.g. less heat been rejected to a hotter environment as Ultimate Heat Sink, or more probability of failure of some components), thus no cliff edge effects are determined, however the use of Temperatures of 10-2 years recurrence versus 10-4 years recurrence will need to be discussed and addressed. |

### Section VII: Structures and Systems Performing Confinement Safety Function

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 126 | | |
| (1) The reactor installation design shall provide for a containment structure and a set of systems and means to ensure the performance of the main safety function of "confinement of releases of radioactive substances to the environment" in accordance with the authorised limits in all operational states and in accident conditions. Besides, the containment shall protect the reactor installation from extreme external events. | COM  NAS | The AP1000 design has a containment building consisting of a steel containment vessel and a seismic Category I shield building. Generic information related to the AP1000 containment type is provided in the AP1000 plant DCD Section 1.1.2 and 1.2.4.1. The conformance with Nuclear Regulatory Commission (NRC) General Design Criteria for reactor containment is presented in DCD Section 3.1.5.  The AP1000 plant containment system is described in DCD in section 6.2. The containment consists of a steel containment vessel and is surrounded by a concrete shield building. The containment is designed to house the RCS and other safety systems. The containment vessel functions as an essential leak tight barrier. In addition, the steel containment performs passive core cooling functions as part of the passive containment cooling system to transfer heat from containment to the ultimate heat sink (the atmosphere). It is protected against malevolent aircraft impact, environmental hazards (e.g., flooding) and postulated missiles from external sources (by the shield building) as well as missiles produced by internal equipment failures.  Containment hydrogen control is discussed in the AP1000 plant DCD Section 6.2.4.  Containment penetrations are isolated as presented in the AP1000 plant DCD Section 3.1. Containment isolation is discussed in the AP1000 plant DCD Section 6.2.3  AP1000 design provides containment structure (see DCD section 3.8) and systems and functions to ensure confinement of releases of radioactive substances to the environment (see DCD section 6.2). External event protection is considered in the containment structural design.  Fulfilment of authorized limits may require further considerations. |
| (2) In order to perform the confinement function the design shall provide for:  1. leaktight structure (containment);  2. systems and means for control of containment environment parameters;  3. systems and means for containment structure isolation;  4. Systems and means for reducing the concentration of radioactive fission products, hydrogen and other substances that could be released in the containment atmosphere during and after accident conditions, including in accidents with fuel melting. | COM | 1. Containment leaktight structure is presented in DCD section 3.8. Parameters credited in Accident Analyses for Containment Leak Tightness can be seen in DCD Table 15.4-4 (0.1% 0 to 24 hours and 0.05% for more than 24 hours).   The reactor containment, containment penetrations and isolation barriers are designed to permit periodic leak rate testing in accordance with General Design Criteria 52, 53, and 54. The containment leak rate test system is designed to verify that leakage from the containment remains within limits established in the technical specifications, Chapter 16.   1. Systems and functions for control of containment environmental parameters are provided in DCD section 6.2. Some of these parameters are controlled by Technical Specifications, 2. Containment isolation system is provided in DCD section 6.2.3. Containment penetrations are isolated according to the provisions of US NRC GDCs 54, 55, 56, and 57 as presented in the AP1000 DCD Section 3.1. 3. Containment Hydrogen Control System is provided in DCD section 6.2.4, and Fission Product Removal and Control Systems are presented in DCD section 6.5. |
| Article 127 |  |  |
| (1) The containment structure and its components, including hermetic access doors, penetrations and isolation devices, shall be designed with sufficient safety margins to withstand static and dynamic loads of internal overpressure and underpressure, temperatures, missiles impact, reaction forces, and of other potential energy sources anticipated to arise as a result of accident conditions, including in accidents with fuel melting. The maximum strength of the containment and its components shall be determined with account being taken of:  1. impacts of extreme external events, including modern passenger aircraft crash;  2. combination of impacts generated by rupture of the reactor coolant boundary pipe with maximum diameter, and a safe shutdown earthquake. | COM | Containment structure and its components are designed with sufficient margins to withstand static and dynamic loads. Loads and load combinations, which are considered in the design are presented in DCD section 3.8.2.3. Consideration of aircraft crash is presented in DCD section 19, appendix 19F, see also article 33(5). |
| (2) The design shall include means for containment structure surveillance in all operational states and accident conditions. | COM | See DCD section 3.1, provisions exist for conducting individual leakage rate tests on containment penetrations. Penetrations are visually inspected and pressure-tested for leak tightness at periodic intervals. Other inspections are performed as required by 10 CFR 50, Appendix J. According to the requirements of 10 CFR 50, Appendix J which dictates a program consisting of a schedule for conducting Type A, B, and C tests shall be developed for leak testing the primary reactor containment and related systems and components penetrating primary containment pressure boundary. The specified maximum allowable containment leak rate is 0.10 weight percent of the containment air mass per day at the calculated peak accident pressure, identified in DCD subsection 6.2.1.  In the AP1000 containment design, the sealing is usually part of the airlock doors, equipment hatches and the other containment penetrations. Regardless of the type, each seal is subject to regular testing and analysis related to the seal performance. Every seal has a design life (the time during which satisfactory performance can be expected for a specific set of service conditions) defined. The tests are run to verify the quality and performance of the seals. For example, Airlock Door Seal and Equipment Hatch Seal Leak Test or Spare Penetration Seal Leak Test are performed. The qualified lives for each individual component (sealing as well) in the equipment hatches and airlocks and all maintenance, surveillance, and replacement programs are followed. |
| Article 128 | | |
| (1) The containment structure and its components shall be designed and constructed to ensure structural integrity testing during commissioning and performing of periodic leaktightness tests over the plant lifetime. The design shall specify requirements to tests and the respective methods and means to conduct the tests. The components located inside the containment shall retain their functional capability after the tests have been conducted. | COM | As presented in DCD section 3.8.2.7, testing of the containment vessel and the pipe assemblies forming the pressure boundary within the containment vessel will be according to the provisions of NE-6000 and NC-6000.  Containment test environment is presented in DCD section 3, Appendix 3D 3D.5.4, which specifies that containment integrity is demonstrated at 1.15 times design pressure.  See DCD section 3.1, GDC 52: The containment system is designed and constructed, and the necessary equipment is provided to permit periodic integrated leakage rate tests according to the requirements of 10 CFR 50, Appendix J. |
| (2) The design shall ensure possibilities to control containment radioactive leakages in case of accidents with fuel melting. | COM | AP1000 design includes severe accident management strategy to ensure that accidents with fuel melting can be managed (see DCD section 19.34) and radioactive leakages to the environment are minimized.  The Radiation Monitoring System, as part of the Post Accident Monitoring provides the capability to monitor plant processes, effluent discharge paths, and areas, under accident and post-accident conditions, to ascertain if there have been significant releases, planned or unplanned, of radioactive materials and to continuously monitor such releases, in addition to monitoring for increased area radiation. According to R.G. 1.97 maintaining containment integrity, including radioactive effluent control is one of the variables that provide information to the MCR operating staff to assess the process of accomplishing or maintaining critical plant safety functions. |
| Article 129 | | |
| (1) The number of penetrations through the containment structure shall be as low as possible. The penetrations design shall meet the same requirements as applied to the containment structure with account taken of possible mechanical, thermal, and chemical effects. | COM | AP1000 design containment has a significantly reduced number of penetrations. The number of normally open containment penetrations is also reduced. The result is a low containment leak rate and a low probability of bypass.  As presented in the DCD section 6.2.3.1.3, the number of pipelines which provide a direct connection between the inside and outside of primary containment during normal operation are minimized.  As presented in the DCD section 3.8.2.1.1, penetrations assemblies are part of the containment vessel, and they have the same requirements as applied to the containment structures. |
| (2) The elastic components of containment penetrations shall be designed to allow individual leak testing, independent of the containment leak rate detection (integral test). | COM | The Containment Leak Rate Test System (see DCD section 6.2.5) provides individual leak testing of the containment penetrations (type B and C) and integral leak rate testing (type A). |
| Article 130 | | |
| (1) To ensure reliable isolation of the containment during accidents, each line that penetrates the containment (whether part of the reactor coolant pressure boundary or directly connected to the containment atmosphere) shall be reliably isolated by at least two isolation valves having independent automatic control, arranged in a series and located as close as practicable to the containment structure outside and inside. | CWO | Containment isolation system is described in DCD section 6.2.3.  The number of penetrations through the AP1000 plant containment has been reduced as a result of the use of passive safety systems and other plant simplifications. Most penetrations are normally closed, and all penetrations use remotely operated valves for isolation that close automatically. Where possible, the containment isolation valves are fail- closed air operated valves which fail to their safe position on a loss of power, loss of signal, or loss of air. See AP1000 plant DCD [2] Section 6.2.3 for additional information.  Piping systems penetrating the containment have containment isolation features. These features serve to minimize the release of fission products following a DBA. Standard Review Plan Section 6.2.4 provides acceptable alternative arrangements to the explicit arrangements given in US NRC GDC 55, 56 and 57. AP1000 plant DCD [2] Table 6.2.3-1 lists each penetration and provides a summary of the containment isolation characteristics. The Piping and Instrumentation Diagrams of the applicable systems show the functional arrangement of the containment penetration, isolation valves, test and drain connections.  Lines that penetrate the containment that are connected to the reactor coolant pressure boundary or to the containment atmosphere have two isolation valves (one inside the containment and one outside the containment) and located as close to the containment as practical.  Containment isolation valves (CIVs), piping between the CIVs, and test connections are not only a part of the Containment System (CNS) isolation system, but an integral part of the process system that penetrates containment. However, these components must comply with the CNS design criteria for the containment boundary, and must be either AP1000 Safety Class A or B. This classification may be higher or lower than the process system’s requirements.  The safety classification of the containment penetrations are the same as the containment itself (AP1000 plant Safety Class B, Seismic Category 1). Also refer to the AP1000 plant DCD [2] Section 6.2.3 and response for Paragraph 6.13.  Acceptable bases for isolation provisions for lines which penetrate the containment boundary shall be in accordance with the following regulatory and code requirements:   * ANS 56.2-1984, Section 3.6 * Regulatory Guide 1.141 * Standard Review Plan (SRP) NUREG-0800 subsection 6.2.4 * Safety Guide 1.11 (Reference 12.1.3.1) as detailed in AP1000 Conformance With SRP Acceptance Criteria * 10CFR50 Appendix A, GDC 55, 56, and 57   Containment isolation is automatically actuated by a safeguards actuation signal, using two-out-of-four coincident logic. The containment isolation actuation is set as low as reasonable without creating potential for spurious trips during normal operations. Containment isolation can also be initiated manually from the MCR. Containment penetrations do not automatically reopen on the resetting of the isolation signal. See subsection 6.2.3 for additional information.  The DAS provides a backup means of actuating risk important containment penetrations.  Isolation of the four PCS instruments lines for containment pressure measurement is demonstrated on a different basis (see further details in DCD section 6.2.3). |
| (2) Each line that penetrates the containment and is neither directly connected to the reactor coolant pressure boundary nor connected directly to the containment atmosphere shall be reliably isolated by at least one containment isolation valve located outside the containment and as close to the containment as is practicable. | COM | Containment isolation system is described in DCD section 6.2.3.  Lines that penetrate the containment and are neither part of the reactor coolant pressure boundary nor connected directly to the containment atmosphere are considered closed systems within the containment and are equipped with at least one containment isolation valve of one of the following types:   * An automatic isolation valve (a simple check valve is not used as this automatic valve) * A locked-closed valve   This valve is located outside the containment and as close to the containment wall as practical. |
| (3) Isolation valves shall retain their operability in all accident conditions. | COM | Containment isolation system is described in DCD section 6.2.3. As presented in the design basis, isolation valves are designed to operate in all accident conditions. |
| Article 131 | | |
| (1) To secure personnel access to the containment premises, provisions shall be made of airlocks and doors with interlocks to ensure that at least one of the doors is closed during all operational states and accident conditions. The same requirements shall be applied when transporting components through the containment structure. | COM | Two personnel airlocks are provided; one located adjacent to each of the equipment hatches, see DCD figure 3.8.2-3. Personnel airlocks are presented in DCD section 3.8.2.1.4. Each airlock has two double-gasketed, pressure-seated doors in series. The doors are mechanically interlocked to prevent simultaneous opening of both doors and to allow one door to be completely closed before the second door can be opened. |
| (2) The design shall consider the capabilities to ensure the functionality of containment airlocks in all accident conditions. | COM | Containment vessel pressure capabilities, incl. airlocks, are summarized in DCD section 3.8.2, Table 3.8.2-2. |
| Article 132 | | |
| The containment design shall include measures and hardware devices to ensure sufficiently low pressure difference between the separate internal compartments not to challenge the integrity of the pressure bearing structure or of other systems with confinement functions, taking into account the pressure and the possible effects in all accident conditions. | COM | As presented in DCD section 6.2.1.2, subcompartments within containment are designed to withstand the transient differential pressures of a postulated pipe break. These subcompartments are vented so that differential pressures remain within structural limits.  DCD section 3.6 describes the application of the mechanistic pipe break criteria (leak-before-break (LBB)), to the evaluation of pipe ruptures. This eliminates the need to consider the dynamic effects of postulated pipe breaks for pipes which qualify for LBB. |
| Article 133 | | |
| (1) The design shall provide for pressure and temperature control systems within the containment for any accidental release of high energy fluids. These systems shall be sufficiently efficient and reliable (including degree of redundancy, independence and diversity) to perform their functions over a long period of time following an accident with fuel melting, taking account of the effects of non-condensable gases. | COM | Passive Containment Cooling System is presented in DCD section 6.2.2. Its functional objective is to reduce the containment temperature and pressure following a loss of coolant accident (LOCA) or main steam line break (MSLB) accident inside the containment by removing thermal energy from the containment atmosphere. The passive containment cooling system also serves as the means of transferring heat to the safety-related ultimate heat sink for other events resulting in a significant increase in containment pressure and temperature. Redundancy, independence, diversity, and autonomy is considered in the system design.  As presented in DCD section 19.40, passive containment cooling is used also in accidents with fuel melting. |
| (2) If a filter venting system is provided for pressure control, the system actuation parameters values and the containment strength shall be dimensioned in a way that the system is not required in the early phase of the accident, taking account of the pressure of the non-condensable gases accumulated in the containment. | N/A | Filtered venting system is not considered for AP1000 design.  For the AP1000 design, emergency containment venting is not typically required due to the loss of containment cooling function but is a severe accident management strategy to relieve containment overpressure Containment venting to the spent fuel pool is available through RNS hot leg suction line MOVs. |
| (3) When a filter venting system is included in the design, it shall not be designed as the principal means of removing the containment residual heat generated as a result of an accident with fuel melting. | N/A | Filtered venting system is not considered for AP1000 design. |
| Article 134 | | |
| (1) The NPP design shall provide for systems to control and cleanup the containment atmosphere, and systems to control the concentration and control of fission radioactive products, oxygen, hydrogen, and other substances, which could be released in the containment during accident conditions. | COM | Fission product Removal and Control Systems are described in DCD section 6.5.  The AP1000 does not include a safety-related containment spray system to remove airborne particulates or elemental iodine. Removal of airborne activity is by natural processes that do not depend on sprays (that is sedimentation, diffusiophoresis, and thermophoresis). These removal mechanisms are discussed in DCD appendix 15B.  Containment Hydrogen Control System is presented in DCD section 6.2.4. |
| (2) The systems and provisions for hydrogen concentration management during accident with fuel melting shall have sufficient capacity to prevent the destruction of the containment as a result of an explosion of combustible gases. Loads resulting from instant burning and detonation of combustible gases that could threaten the containment integrity and leaktightness shall be practically eliminated. | COM | Containment Hydrogen Control System is presented in DCD section 6.2.4. System ensures hydrogen control during and following a degraded core or core melt scenarios (provided by hydrogen igniters). In addition, non-safety-related passive autocatalytic recombiners (PARs) are provided for defense-in-depth protection against the buildup of hydrogen following a loss of coolant accident.  As presented in DCD section 19.34.2.3, containment failure from a directly initiated detonation wave is not considered to be a credible event for the AP1000 containment. There are no ignition sources of sufficient energy to directly initiate a detonation in the AP1000 containment. Deflagration to detonation transition (DDT) is the only likely mechanism to produce a detonation in the AP1000 containment.  Hydrogen mixing and combustion analyses are presented in DCD section 19.41 to confirm that there is sufficient capacity for hydrogen control. |
| (3) The systems for containment atmosphere cleaning up shall have adequate components' reliability and redundancy to ensure the required efficiency of the system on the assumption of a single failure. | COM | Removal of airborne activity is by natural processes that do not depend on sprays (that is sedimentation, diffusiophoresis, and thermophoresis). These removal mechanisms are discussed in DCD appendix 15B. Thus, there is no need for consideration of single failures (however, AP1000 design includes non-safety active system for containment spray, see DCD section 6.5). Thus, high reliability of the atmosphere cleaning is ensured. |
| Article 135 | | |
| The selection of coatings and thermal insulation, and methods for their application on SSCs inside the containment, shall ensure the fulfilment of their safety functions and shall minimise interference with other safety functions in the event of degradation of their integrity. | COM | Thermal insulation is described in DCD section 6.1.1.6. Most of the engineered safety features insulation used in the AP1000 containment is reflective metallic insulation. Fibrous insulation may be used if it is enclosed in stainless steel cans.  Regarding coatings inside the containment, see DCD section 6.1.2.1. The AP1000 design considers the function of the coatings, their potential failure modes, and their requirements for maintenance. Table 6.1-2 in the DCD lists different areas and surfaces inside containment and on the containment shell that have coatings, their functions, and to what extent their coatings are related to plant safety.  Air ingestion, vortexing, and debris blockage are not significant concerns for the AP1000. Containment recirculation includes sump screens that conform to the criteria specified in Regulatory Guide 1.82., thus addressing Generic Safety Issue (GSI) 191 and Generic Letter 2004-02. |

### Section VIII: Supporting Safety Systems

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 136 | | |
| The NPP design shall provide for supporting safety systems fulfilling auxiliary services of supplying safety systems with fluids and energy, and maintaining their operational conditions over a justified period of time in all operational states and accident conditions. | COM | Due to the passive features of the AP1000 design, the number of supporting safety systems needed for accident management is limited. Support safety systems fulfills their design basis to provide fluid and energy in all operating states and accident conditions. |
| Article 137 | | |
| (1) The supporting safety systems shall be designed with adequate components' reliability and redundancy to ensure the necessary effectiveness on the assumption of a single failure, independent of the initial state. | COM | Due to the passive features of the AP1000 design, the number of supporting safety systems needed for accident management is limited. Adequate reliability and redundancy are applied in the system design. This is confirmed with probabilistic safety analysis, see DCD section 19. |
| (2) The degree of functional reliability of the supporting systems shall be sufficient to meet the required reliability criteria of the respective safety system. | COM | Due to the passive features of the AP1000 design, the number of supporting safety systems needed for accident management is limited. Functional reliability of the supporting systems is sufficient to meet the required reliability criteria of the respective safety system. This is confirmed with probabilistic safety analysis, see DCD section 19. |
| (3) The systems design shall provide a possibility for testing of their functional capability and for failure indication. | COM | Testing and failure indications are considered in the support system design, and they are described in the respective system descriptions in the DCD. |
| (4) The fulfilment of supporting functions shall have priority over the supporting systems own protections, if this will not aggravate the safety consequences. The design shall specify the uninterruptible own protections of the components of the supporting safety systems. | CWO | Due to the passive features of the AP1000 design, number of supporting safety systems needed for accident management is limited, since main safety functions are performed by passive systems, thus active components are not classified as safety related to perform safety functions (they are included in the Defense in Depth type of Systems, thus not safety Related), for the previous reason the need to preclude their own protections is not as relevant and is to be analyzed only in for Probabilistic Analyses. |
| Article 138 | | |
| (1) The design shall include emergency power supply systems for the SSCs important to safety, in the event of loss of off-site power, capable of performing their functions in all operational states and accident conditions, with the assumption of a single failure and common cause failure. | COM | Due to the passive features of the AP1000 design, the need for power supply in accident management is limited. The Class 1E DC and UPS system (IDS) provide reliable power for safety-related equipment.  Power supply systems and their functions in operational states and accident conditions are presented in DCD section 8.  For Active Defense-in-Depth (DiD) systems: When ac power is available, the AP1000 plant passive systems can be supplemented with simple, active Defense-in-Depth (DiD) systems and equipment.  The active DiD systems use reliable and redundant active equipment, supported by the use of **DiD diesels** to facilitate their functions when offsite ac power is not available. These simple, active systems, structures and components (SSCs) are optimized for their normal operating functions.  The active systems provide investment protection and reduce the overall risk to the plant owner and the public by minimizing the demand on the passive safety features**. While important to the safe operation of the plant**, the active systems are not necessary for the safe shutdown of the reactor following a design basis event. The DiD system design includes sufficient redundancy so that the most probable single failures cannot result in the loss of the DiD functions, for example by including **two 100 percent capacity trains**. The DiD SSCs are controlled by the plant control system, while the passive safety systems are actuated by the protection and safety monitoring system.  The consideration of single failures and common cause failures are considered to the extent necessary. |
| (2) The design solutions against common cause failures, including those resulting from external events, shall include an alternative (diverse) emergency source of alternate power supply (stationary or mobile), qualified to operate under conditions of extreme external events of natural origin. | COM | Due to the passive features of the AP1000 design, the need for power supply in accident management is limited. The Class 1E DC and UPS system (IDS) provide reliable power for safety-related equipment.  Alternate power supply can be provided with two ancillary ac diesel generators. The ancillary generators are not needed for refilling the PCS water storage tank, spent fuel pool makeup, post-accident monitoring or lighting for the first 72 hours following a loss of all other ac sources. The design of equipment anchorages is consistent with the SSE design of equipment anchorages of seismic Category I items and there is no spatial interaction with any other non-seismic SSC that could adversely interact to prevent the functioning of the post-72 hour SSCs following an earthquake; no dynamic qualification of the active equipment is necessary. Features of this structure which protect the function of the ancillary generators are analyzed and designed for Category 5 hurricanes, including the effects of sustained winds, maximum gusts, and associated wind-borne missiles. |
| (3) To ensure the required reliability of the emergency power supply for a long period of time (not less than 72 hours) following accident conditions, the design shall provide for:  1. sufficient capacity of the DC power supply sources or a possibility for their recharging;  2. sufficient stock of fuels and consumables for the emergency and alternative AC power supply sources. | COM | Due to the passive features of the AP1000 design, the need for power supply in accident management is limited. The Class 1E DC and UPS system (IDS) provide reliable power for safety-related equipment.  As presented in the DCD section 8.1.4.2.1, The Class 1E DC and UPS system has sufficient capacity to achieve and maintain safe shutdown of the plant for 72 hours following a complete loss of all ac power sources without requiring load shedding for the first 24 hours.  Two ancillary ac diesel generators, located in the annex building, provide ac power for Class 1E post-accident monitoring, MCR lighting, MCR and I&C room ventilation, and pump power to refill the PCS water storage tank and the spent fuel pool, when all other sources of power are not available. Fuel tank holds sufficient fuel for 4 days of operation, thus allowing to reach 7 days. |
| Article 139 |  |  |
| (1) The design shall make provisions for fire detection and fire extinguishing systems to prevent fire-induced common cause failures in the safety systems and to automatically fulfil the specified functions. The fire extinguishing systems shall be capable of automatic actuation. | COM | Fire protection systems are presented in DCD section 9.5.1. Design basis of fire protection systems includes detection of fires and prevention of fire propagation with automatic fire extinguishing systems. |
| (2) The fire safety measures shall ensure defence in depth by preventing fire, fast detection and extinguishing of any fire, ensuring the structure stability in the event of fire, limiting the fire and smoke propagation and the fire consequences, creating conditions for occupants evacuation and for safety of the rescue teams. To achieve those objectives:  1. the building structures shall be conservatively designed as fire resistant with consideration of internal and external fires;  2. the internal structures and components shall be of fire response class A1 or A2;  3. the fire load shall be kept at the practically achievable minimum;  4. the power unit shall be subdivided into fire protection sections through fire protection barriers with adequate fire resistance, capable of preventing spread of smoke and heat from fires considered in the design;  5. the characteristics of the fire detection and fire extinguishing systems (reliability, independence, capacity and qualification) shall be selected with consideration of the fire hazard resulting from the analysis, required under Article 77;  6. the required protected areas, safe areas, evacuation routes and fire evacuation exits shall be provided;  7. conditions for urgent fire extinguishing shall be ensured: external and internal water supply for fire extinguishing, fire routes and access of the rescue teams. | COM/OR  NAS | Defense-in-depth is applied in the fire safety measures, as presented in the fire protection design basis, see DCD section 9.5.1.1.   1. Architectural and Structural Features are considered in DCD section 9.5.1.2.1.1. 2. Fire response class A1 or A2 may require further consideration in the design. This class A1 and class A2 need to be clarified. 3. As presented in DCD section 9.5.1.1.1, limiting the quantities of combustibles and sources of ignition is part of the design basis. The design and the procedures applied by the owner, Owner Operational Requirement, shall prevent fire initiation by controlling, separating, and limiting the quantities of combustibles and sources of ignition. 4. As presented in DCD section 9.5.1.1.1, isolation of combustible materials and limitation of the spread of fire by subdividing plant buildings into fire areas separated by fire barriers is part of the design basis. 5. As presented in DCD section 9.5.1.2.1.2, fire detection and alarm systems are provided where required based on the fire protection analysis and consideration of the type if hazard, combustible loading, the type of combustion products, and detector response characteristic. Automatic fire suppression systems are provided with consideration of the unique aspects of each application, including building characteristics, materials of construction, environmental conditions, fire area contents, and adjacent structures. 6. As presented in DCD section 9.5.1.2.1.1, firefighting personnel access routes and life safety escape routes are provided for each fire area. 7. As presented in DCD section DCD section 9.5.1.2.1, access routes are provided, and water supply is ensured. |

### Section IX: Other SSCs Important to Safety

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 140 | | |
| 1) The design of the steam generators and steam lines system (steam supply system), the steam generators feedwater system and the turbine and generators system for the nuclear power plant shall be such as to ensure that the appropriate design limits of the reactor coolant pressure boundary are not exceeded in all operational states or in accident conditions. | COM | It is ensured that reactor coolant pressure boundary is not exceeded in operational or in accident states, this is confirmed with deterministic safety analyses, see DCD section 15. |
| (2) The design of the steam supply system shall provide for appropriately rated and qualified steam isolation valves capable of closing under the specified conditions in operational states and in accident conditions. | COM | As presented in DCD section 10.3.1, the design includes main steam isolation valve (MSIV) and associated MSIV bypass valve on each main steam line from its respective steam generator. Applicable ASME code class is used for these valves. |
| (3) The steam supply system and the steam generators feedwater system shall be of sufficient capacity and shall be designed to prevent anticipated operational occurrences from escalating to accident conditions. | COM | Sufficient capacity of the steam supply and feedwater system is included to prevent AOO’s from escalating to accident conditions. DCD table 15.0-8 presents non-safety related systems and equipment used for mitigation of accidents. |
| (4) The design of the turbine and generators system shall be provided with appropriate protection such as overspeed protection and vibration protection, and measures shall be taken against possible impacts of missiles generated by component destruction on SSCs important to safety. | COM | Turbine-Generator design basis is presented in DCD section 10.2. Design includes necessary protections, including overspeed protection and alarms for high vibration. Turbine missiles are assessed in DCD section 3.5. |
| Article 141 | | |
| Overhead transport and lifting equipment that is used for the SSCs important to safety, or for transport of heavy loads in close proximity to such SSCs shall be designed so as to:  1. prevent the movement of loads exceeding the design load capacity;  2. prevent, using conservative design measures, any unintentional dropping of loads that could affect SSCs important to safety;  3. be used only in specified operational states by means of safety interlocks;  4. be seismically qualified. | COM | Overhear Heavy Load Handling Systems are presented in DCD section 9.1.5.   1. Interlocks are designed for hoist overload. 2. 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. 3. As presented in the design basis, 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. Limit switches are designed to initiate protective responses to various events, such as hoist overtravel and overspeed. 4. Polar crane, Cask Handling Crane, Equipment Hatch Hoist and Maintenance Hatch Hoist are qualified to Seismic Category I. |
| Article 142 | | |
| The design basis for any compressed air system that serves an item important to safety shall specify the quality, flow rate and cleanness of the air to be provided. | COM | Compressed Air and Instrument Air System is presented in DCD section 9.3.1. The compressed and instrument air system serves no safety-related function other than containment isolation and therefore has no nuclear safety design basis except for containment isolation where the fail-safe principle is applied in case of loss of air. Table 9.3.1-1 in DCD presents the list of components, which are operated by air. |
| Article 143 | | |
| Adequate protection against lightnings of all buildings and working areas on the NPP site shall be ensured in all operational states and accident conditions. | COM | Lightning protection is presented in DCD section 8.3.1.1.8. The lightning protection system is provided for the protection of exposed structures and buildings housing safety-related and fire protection equipment in accordance with NFPA 780. |

### Section X: District Heating System

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 144 | | |
| (1) When the NPP is coupled with heat utilisation unit for district heating, the design shall include measures for practical elimination of transport of radionuclides from the NPP systems to the supply system coolant of the district-heating unit in all operational states and accident conditions. | N/A | AP1000 Standard Design or Reference Plant do not consider District Heating/Heat Generation. Nevertheless, in case heat production were requested, this might be feasible but will request a specific scope to be developed. |
| (2) The measures for preventing radioactive contamination of the supply system coolant shall be identified considering the following requirements:  1. The plant heat shall be transferred to the intermediate coolant through leak tight heat-exchangers;  2. The heat-up of the supply system coolant by the intermediate coolant shall be performed by means of heat-exchangers;  3. The intermediate coolant pressure shall be lower than the supply system coolant pressure. | N/A | AP1000 Standard Design or Reference Plant do not consider District Heating/Heat Generation. Nevertheless, in case heat production were requested, this might be feasible but will request a specific scope to be developed. |
| Article 145 | | |
| (1) Means for isolation of the supply system coolant from the intermediate coolant heat exchanger shall be provided to prevent accident-related ingress of radioactive substances in the intermediate coolant. | N/A | AP1000 Standard Design or Reference Plant do not consider District Heating/Heat Generation. Nevertheless, in case heat production were requested, this might be feasible but will request a specific scope to be developed. |
| (2) The heat exchangers used for heating of the supply system coolant shall be located on the NPP site. | N/A | AP1000 Standard Design or Reference Plant do not consider District Heating/Heat Generation. Nevertheless, in case heat production were requested, this might be feasible but will request a specific scope to be developed. |

### Section XI: Radioactive Waste Management

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 146 | | |
| (1) The radioactive waste (RAW) management systems shall be designed based on analysis and assessment of the composition and quantities of solid and liquid RAW and the gaseous radioactive substances generated in all operational states and accident conditions. | COM | Radioactive waste management systems are described in DCD section 11. Waste systems are designed based on composition and quantities of liquid, solid and gaseous waste assessments, see DCD tables 11.2-1 (liquid waste) and Table 11.4-1 (solid waste). Regarding gaseous waste, capacities are presented in DCD section 11.3.1.2.1.  See specific assessment in BGP-GW-GL-205 [8]. Per discussion with KNPP-NB, see L.WEC\_KNP\_230019 [27], on the Role of SERAW Bulgarian State Enterprise for “Radioactive Waste”. It was Clarified by KNPP-NB that SERAW will be responsible for the predisposal treatment and Conditioning of Radwaste (e.g., Volume Reduction, Immobilization, Waste Packaging for Pre-Disposal conditioning) if the radwaste (e.g., Resins and Liquids) to be delivered to SERAW agreed to the Radwaste that can be accepted by SERAW. In this aspect KNPP-NB requested Westinghouse to provide data on our waste streams to confirm their acceptability by SERAW, this was addressed by transmitting the document BGP-GW-GEH-001[29] as attachment 1 to L.WEC\_KNP\_230025 [28].  Envisaged SERAW activities will preclude the need to include treatment systems in a Site Specific Radwaste Treatment Facility (SRTF) and possibly even the need to consider the need for one (unless some additional storage is required). |
| (2) The systems for management of liquid and gaseous radioactive discharges to the environment shall be designed so that their quantities and concentrations are kept as low as reasonably achievable in all operational states and within the specified dose limits for the occupational exposure of the personnel and the dose limits for the population. | COM | As presented in DCD section 11.2.1.2.4, the liquid radwaste system provides the capability to reduce the amounts of radioactive nuclides released in the liquid wastes using demineralization and time delay for decay of short-lived nuclides.  As presented in DCD section 11.3.1.2.1.2, the gaseous radwaste system is designed to reduce the controlled activity releases in support of the overall AP1000 release goal.  See specific assessments in BGP-GW-GL-202[7] and BGP-GW-GL-205 [8]. |
| Article 147 | | |
| (1) The NPP design shall include systems for preliminary treatment and temporary storage of liquid RAW in a condition suitable for transportation and further treatment. | COM | The liquid radwaste system provides (see DCD section 11.2) treatment and temporary storage of liquid RAW, which is suitable for transportation and further treatment.  See response to article 146. |
| (2) The NPP design shall include facilities for temporary storage of solid RAW, equipped with automatic means for handling. | COM | The solid waste management system (see DCD section 11.4) includes equipment for temporary storage of solid RAW, with automatic means for handling.  See response to article 146. |
| (3) The RAW storage compartments shall be watertight and provided with systems for ventilation, decontamination, fire detection and fire extinguishing. | COM | Ventilation systems for waste buildings are presented in DCD 9.4.  Protection against flooding is presented in DCD section 3.4.  Provisions for decontamination of potentially contaminated areas are considered as a part of ALARA principle, see DCD section 12.1.2.3.  Fire detection and fire extinguishing principles are presented in DCD 9.5.1.  See response to article 146. |
| (4) The design shall specify the way for management of large quantities of liquid RAW generated in accident conditions. | OR/NAS | Abnormal conditions, such as high primary coolant system leakage or steam generator tube leakage, are considered in the liquid radwaste system design, see DCD section 11.2.1.2.3.  This requirement will need to be further clarified and discussed. |
| Article 148 | | |
| (1) The NPP design shall ensure maintaining of the volume and activity of the generated liquid RAW as low as reasonably achievable through the use of effective cleanup systems and multiple use of radioactive fluids, leakage prevention in systems containing radioactive fluids, and reduction of the frequency of events that require significant decontamination measures. | COM | As presented in DCD section 11.2.1.2.4, the liquid radwaste system provides the capability to reduce the amounts of radioactive nuclides released in the liquid wastes using demineralization and time delay for decay of short-lived nuclides.  See also application of ALARA-principle, DCD section 12.1. |
| (2) The plant RAW management systems shall be designed with account taken of the requirements to the subsequent stages of their safe management. | N/A | This is analyzed in the Assessment of the AP1000 Plant for the Bulgarian Regulation Related to Safe Management of Radioactive Waste [8]. There it is recognized that selected waste disposal conditions the Radwaste Treatment facilities by Imposing Radwaste Acceptance Criteria, however these treatment facilities are considered out of the scope of this assessment as Site Radwaste Treatment Facility (SRTF) is not included in the standard design and is not considered at this point as part of the project.  See also discussion on SERAW role in article 146. |

### Section XII: Handling and Storage of Nuclear Fuel

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 149 | | |
| The NPP design shall include SSCs for handling and storage of non-irradiated fuel designed to:  1. prevent criticality by a sufficient margin, even under the most adverse conditions, by ensuring appropriate physical means or processes, such as geometrically safe configurations, and characteristics of the components and medium;  2. permit appropriate fuel acceptance test, maintenance, periodic inspection and testing of components important to safety;  3. ensure control of the storage conditions;  4. minimise the possibility of damage or unauthorised access to the nuclear fuel;  5. prevent fuel assembly drop during transportation;  6. prevent inadvertent dropping of heavy objects upon the fuel assemblies. | COM | Fuel storage and handling is presented in DCD [2] section 9.1., see also assessment BGP-GW-GL-204 [30]. These systems ensure that the integrity and properties of the fuel are maintained at all times during fuel handling and storage.  The New Fuel Storage is discussed in the AP1000 DCD Section 9.1.1.  Spent Fuel Storage is discussed in the AP1000 DCD Section 9.1.2.  The AP1000 plant DCD [2] Section 9.1.4 discusses the Light Load Handling System (Related to Refueling).  Safety evaluations for the above are reported in the AP1000 plant DCD Sections 9.1.1.3, 9.1.2.3 and 9.1.4.3.   1. New and spent fuel rack design ensures subcriticality during spent fuel storing. Criticality during fuel handling operations is prevented by the geometrically safe configuration of the fuel handling equipment. 2. Appropriate tests, maintenance and periodic inspections are considered. 3. New and spent fuel storages are presented in DCD sections 9.1 . Proper storing conditions are ensured. 4. The possibility of fuel damage is minimized by fuel design, by ensuring proper conditions for fuel storing and handling and by security features. Fuel handling accidents are evaluated in DCD section 15.7.4. 5. The fuel handling system is presented in DCD section 9.1.4. One of the design bases is to have provisions to avoid dropping or jamming of fuel assemblies during transfer operation. 6. As presented in DCD section 9.1.5.1, to the extent practicable, heavy loads are not carried over or near safety-related components, including irradiated fuel and safe shutdown components. |
| Article 150 | | |
| (1) The design of SSCs used for spent fuel storage and handling shall be aimed at practical elimination of accidents with large or early radioactive release, including accidents with fuel melting. | COM | Practical elimination of accidents is considered in separate report “AP1000 Plant Methodology for Demonstration of Practical Elimination” [5]. |
| (2) In addition to the requirements applicable to the fresh fuel storage, the spent fuel storage and handling SSCs design shall take into consideration the following additional measures and means:  1. Availability of sufficiently reliable and, if needed, diverse, residual heat removal systems and means in all operational states and accident conditions.  2. Measures to prevent unacceptable handling stresses on the fuel assemblies;  3. Means for safe storage of untight or damaged fuel assemblies or fuel elements;  4. Systems for local ventilation and other means for radiation protection;  5. Means for identification of the fuel assemblies. | COM | 1. See reference [12]. Spent fuel pool cooling is presented in 9.1.3.1.3. If the spent fuel pool cooling system is unavailable, spent fuel cooling is provided by the heat capacity of the water in the pool.   The spent fuel pool cooling system includes safety-related connections from the passive containment cooling water storage tank in the passive containment cooling system to establish safety-related makeup to the spent fuel pool following a design basis event including a seismic event. In addition to the safety-related water sources, makeup water is also obtained from the passive containment cooling ancillary water storage tank. Water from this tank can be pumped by the passive containment cooling system recirculation pumps either to the passive containment cooling water storage tank (and then gravity fed to the spent fuel pool), or directly to the spent fuel pool.   1. Interlocks are designed to ensure unacceptable handling, see DCD section 9.1.4.3. 2. Spent fuel storage includes storage locations for five defective fuel assemblies, see DCD section 9.1.2.1. 3. During fuel handling operations, a ventilation system removes gaseous radioactivity from the atmosphere above the spent fuel pool, see DCD section 9.4.3 for radiologically controlled area ventilation system and section 11.5 for process radiation monitoring. 4. As presented in DCD section 15.4.7, each fuel assembly is marked with an identification number and loaded in accordance with a core loading diagram to reduce the probability of core loading errors. During core loading, the identification number is checked before each assembly is moved into the core. Serial numbers read during fuel movement are subsequently recorded on the loading diagram as a further check on proper placement after the loading is completed |
| (3) For reactors using a water pool system for storage of irradiated fuel, the design shall provide for the following:  1. Means for monitoring and controlling the water parameters in the pool (including level, chemistry and activity), as well as means for leak detection;  2. Means and measures for maintaining the integrity of the pool's civil structure, including against extreme external events;  3. Measures to prevent emptying the pool as a result of syphon effect in the event of a pipe break;  4. Means to control the concentration of the soluble neutron absorber. | COM | 1. The spent fuel pool cooling system is presented in DCD 9.1.3, which includes cooling and purification. The Spent fuel system (SFS) piping includes individual sampling points, Fuel Storage Pool Boron Concentration is under technical specification 3.7.11, see DCD Chapter 16. The pool leak detection system is zoned to allow identification of the area of the pool liner, which is leaking, even for very small leaks. 2. As presented in DCD section 9.1.2.2, the spent fuel storage facility is designed to the guidelines of ANS 57.2. The spent fuel storage facility is located within the seismic Category I auxiliary building fuel handling area. The walls of the spent fuel pool are an integral part of the seismic Category I auxiliary building structure. The facility is protected from the effects of natural phenomena such as earthquakes, wind and tornados, floods (Section 3.4), and external missiles. 3. As presented in DCD section 9.1.2.2, pipes which discharge into the spent fuel pool include a siphon break between the normal water level and the level of the spent fuel cooling system pumps' suction connection. 4. As presented in DCD section 9.1.3.2, the spent fuel pool is initially filled for use with water having a nominal boron concentration of 2700 ppm. Demineralized water can be added for makeup purposes, including replacement of evaporative losses, from the demineralized water transfer and storage system. Boron may be added to the spent fuel pool from the chemical and volume control system. See assessment in BGP-GW-GL-204 [30] |
| (4) The design and the safety assessment shall confirm capacity of the structures for storing of irradiated fuel and consider the capability at any time to completely remove the fuel from the reactor core. | COM | Design and safety assessment confirms capacity of the structure for storing of fuel and capabilities to remove the fuel completely from the core, see DCD section 9.1.2. |

### Section XIII: Radiation Protection

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 151 | | |
| (1) To ensure radiation protection, the NPP design shall identify all real and potential sources of ionising radiation and shall provide measures for ensuring the necessary technical and administrative control over their use. | COM | Radiation protection and how ALARA-principle is applied is presented in DCD section 12.  Radiation sources are presented in DCD section 12.2. |
| (2) (amended - SG No. 37/year 2018) The requirements with regard to the classification of zones and premises, radiation monitoring, the personal protective equipment and the access control are established by a different regulation under Article 26, para 2 of the SUNEA. | NAS | Requirement is assessed in connection of SUNEA separately, see assessment of the Act on safe use of nuclear energy [6]. |
| Article 152 | | |
| To keep the exposure of personnel and public as low as reasonably achievable during the plant operation, the design of the reactor coolant system shall arrange for:  1. Use of structural materials with minimum content of chemical elements with high activation cross-section and producing long-lived radioactive corrosion products;  2. Coolant purification from fission and corrosion radioactive products;  3. Water chemistry control;  4. Minimum length of the pipelines with a minimum number of isolation valves and connections;  5. Leak-tightness testing of operating components;  6. Decontamination of SSCs outer and inner surfaces;  7. Prevention of uncontrolled radioactive leaks in the NPP premises. | COM | ALARA principle is summarized in DCD section 12.1, including items 1-7 in this requirement. See also assessment in BGP-GW-GL-201 [7] |
| Article 153 | | |
| (1) Shielding shall be designed in a conservative way, taking into account the build-up of radionuclides over the plant lifetime, and the potential loss of shielding efficiency due to the effects of interactions of neutron and gamma rays with the shielding. | COM | Shielding principles are presented in DCD section 12.3.2. Shielding calculations are performed to ensure that sufficient shielding is available over the plant lifetime. |
| (2) The buildings, premises and components, which may be contaminated with radioactive substances, shall be designed in a way that allows easy decontamination by chemical or mechanical means. | COM | As presented in DCD section 12.1, provisions are made for decontamination of potentially contaminated areas and components, see also as an example consideration for Coating in DCD 6.1.2.1.6.  The AP1000 plant annex building includes a hot machine shop for servicing radiological control area equipment. The hot machine shop includes decontamination facilities including a portable decontamination system that may be used for decontamination operations throughout the nuclear island (AP1000 plant DCD [2] Section 1.2.5).  The health physics area contains the personnel contamination monitoring equipment, decontamination shower facilities, and first-aid equipment (AP1000 plant DCD Section 12.5.2.2  See also assessment in BGP-GW-GL-201 [7] |
| (3) The personnel access to premises of high contamination level shall be controlled by means of locking devices with interlocks and indication for actuation and for inoperability. | COM | As presented in DCD section 12.1, provisions are made for restrictions and control of access to the various radiation zones |
| Article 154 | | |
| (1) Shielding shall be designed in a conservative way, taking into account the build-up of radionuclides over the plant lifetime, the potential loss of shielding effectiveness due to the effects of interactions of neutron and gamma rays with the shielding, due to reactions with other materials, decontamination solutions, and the expected temperature effects. | COM | Shielding principles are presented in DCD section 12.3.2. Shielding calculations are performed to ensure that sufficient shielding is available over the plant lifetime. The thickness of each shield wall surrounding radioactive equipment is determined by approximating as closely as practicable the actual geometry and physical condition of the source or sources. |
| (2) The choice of shielding materials shall be made on the basis of the nature of the ionizing radiation, shielding, mechanical and other properties of materials and spatial limitations. | COM | General principles for section of shielding materials are presented in DCD section 12.3.2.2. Materials used in shielding typically include lead, steel, water, and concrete. The material used for most of the plant shielding is ordinary concrete with a bulk density of approximately 140 lb/ft3. Whenever poured-in-place concrete has been replaced by concrete blocks, an equivalent shielding basis as determined by the density of the concrete block is selected. Steel is used as shielding in the chemical and volume control system and other modules, as well as around the reactor vessel flange at the floor of the refueling cavity. Water is used as the primary shield material for areas above the spent fuel storage area and refueling cavity during refueling operation. |
| Article 155 | | |
| (1) The plant design shall provide ventilation systems to:  1. prevent dispersion of gaseous radioactive substances in the plant premises;  2. reduce and maintain airborne concentrations in plant premises below the authorised limits and as low as reasonably achievable in all operational states and design basis accidents;  3. ventilate the air in premises containing inert or noxious gases. | COM | Radiologically controlled area ventilation system is presented in DCD section 9.4.3. Design basis of the system covers items 1-3 in this requirement. |
| (2) The ventilation system design shall take into account the following factors:  1. Mechanisms of thermal and mechanical mixing;  2. Limited efficiency of dilution in reducing airborne contamination;  3. Extracting the air from areas of potential contamination at points near the source of contamination;  4. Ensuring adequate distance between exhaust air discharge points and the air intake points;  5. Providing a higher pressure in the less contaminated zones in comparison with the zones of higher contamination level;  6. Preventing the spread of flue gases and combustion products to neighbouring premises. | COM | Radiologically Controlled Area Ventilation System (see DCD section 9.4.3) is designed to ensure ventilation to maintain sufficient temperature in the equipment rooms, maintain airborne radioactivity in the access areas at safe level for personnel, maintain airflow from lower potential airborne contamination to areas of higher potential contamination, maintain negative pressure to prevent radioactive releases to the environment and automatically isolate buildings and start filtration system if high radioactivity is detected.  If smoke is detected in the supply or exhaust air ducts, an alarm is initiated in the main control room. In the event of a fire, local fire dampers automatically isolate the HVAC ductwork penetrating the fire area when the local air temperature exceeds predetermined setpoint. |
| Article 156 | | |
| (1) The design shall provide for ventilation and air cleaning systems for discharge of gaseous radioactive substances to the environment. | COM | DCD chapter 11.3.3 describes atmospheric pathways for radioactive releases. Ventilation and air cleaning systems are provided for discharge of gases radioactive substances to the environment, see DCD chapter 9.4.1. |
| (2) The filters of the air cleaning systems shall be sufficiently reliable to perform their function with the necessary decontamination factor in all operational modes. The design shall provide means to test their efficiency. | COM | Filters are designed in accordance with the performance requirements presented in DCD 9.4.1. As presented in DCD section 12.3.3.5, the guidance and recommendations of Regulatory Guide 1.140 concerning maintenance and in-place testing provisions for atmospheric cleanup systems, air filtration, and adsorption units are used as a guide in the design of the various ventilation systems. |
| Article 157 | | |
| (1) Provisions shall be made in the design for an automated system for radiation monitoring in the rooms and at the NPP site, and a system for radiation monitoring in the precautionary action zone and the surveillance zone. These systems shall ensure the collection and processing of information on the radiation conditions, on the effectiveness of protective barriers, on the radionuclides activity, and information necessary to predict changes in the radiation conditions in all operational states and accident conditions. | COM | Radiation monitoring system is presented in DCD section 11.5, which includes the functions presented in this requirement. |
| (2) The equipment of the automated system for radiation monitoring shall enable the implementation of:  1. Process radiation monitoring;  2. Individual dosimetry monitoring;  3. Radiation monitoring in the work rooms and at the NPP site;  4. Area monitoring for limiting the spread of radioactive contamination. | COM | Radiation monitoring system is presented in DCD section 11.5, which includes the functions presented in this requirement. |
| (3) The laboratory methods and technical means of the system for radiation monitoring shall ensure measurement of the human induced radionuclides content in soil, water, deposits, vegetation, water flora and fauna, and agricultural products. | OR | Owner is responsible for off-site radiation monitoring. |

## CHAPTER 7 – CONSTRUCTION AND COMMISSIONING

### Section I: General Requirements

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 158 | | |
| The operating organisation shall exercise control over the implementation of the design, construction and installation works, and over the quality of used materials, structures and components assisted by its own organisational structure and in compliance with the requirements of the regulatory framework. | OR | Requirement for the Owner. |
| Article 159 | | |
| During the construction and commissioning, the NPP site shall be monitored, guarded and maintained so as to protect SSCs, to support the testing stage and to maintain consistency with the technical design and the safety analyses. | COM | Quality assurance program is summarized in DCD section 17. |
| Article 160 | | |
| The SSCs supplied to the plant shall be manufactured under quality assurance programmes that include inspections of the technological cycle, cleanliness, calibration and verification of operability. | COM | Quality assurance program is summarized in DCD section 17. |
| Article 161 | | |
| (1) The operating organisation shall ensure designer supervision by the NPP designer to provide technical assistance. | OR | Requirement for the Owner. |
| (2) The fabrication of the structures and components at the NPP site, construction methods, installation works, single tests and inspections during the construction stage shall be concurred with the NPP designer. | COM | Quality assurance program is summarized in DCD section 17. Initial test program is presented in DCD section 14. |
| Article 162 | | |
| (1) The construction and installation works and the single tests of SSCs important to safety shall be carried out in accordance with written procedures that contain the measures to ensure compliance with the safety requirements, requirements for quality assurance, and requirements for the industrial safety of the personnel. | COM | Quality assurance program is summarized in DCD section 17. Initial test program is presented in DCD section 14. |
| (2) The activities of the suppliers shall be carried out in accordance with procedures, specifications and drawings with specific requirements for quality assurance. | COM | Quality assurance program is summarized in DCD section 17. |
| Article 163 | | |
| (1) During the construction and commissioning the operating personnel shall profit from the opportunity to receive on-the-job training and thus shall be introduced to the construction and installation solutions, the testings of SSCs and the NPP as a whole and the results thereof, validation of the operational and organisational procedures on maintenance, surveillance and inspection, access to work and management of non-compliances. | OR | Requirement for the Owner. |
| (2) All site personnel, including suppliers and contractors participating in the construction and installation works and the commissioning shall be trained to develop safety culture in compliance with Articles 24 and 25. | OR/COM | Training will be provided to develop safety culture.  Westinghouse and its employees receive training and pledge commitment to Nuclear Safety Culture understood as “the core values and behaviors resulting from a collective commitment by leaders and individuals to emphasize safety over competing goals to ensure protection of people and environment.” |
| Article 164 | | |
| (1) The SSCs constructed, supplied and installed shall be compared to their design characteristics during construction and commissioning. | COM | Quality assurance program is summarized in DCD section 17, and Initial Test Program in DCD chapter 14 main objective is to demonstrate that the plant has been constructed as designed |
| (2) Maintenance shall be performed on structures and components that could experience degradation of their characteristics during construction. The maintenance during commissioning shall comply with the same requirements as during operation. | OR/COM | Maintenance shall be performer by the owner to the extent necessary, for structures and components that could experience degradation during construction. |
| (3) Initial control shall be exerted on SSCs that will have subsequent metal control in the future. | COM | The principles for inspections, tests, analyses, and acceptance criteria (ITAAC) are presented in DCD section 14.3.2.2. |
| (4) Adequate actions shall be taken to prevent foreign materials and dirt from entering into exposed and unprotected components. | COM | Quality assurance program is summarized in DCD section 17.  AP1000 design includes several technical solutions and administrative actions to minimize the possibility of the foreign objects entering exposed and unprotected components. |
| Article 165 |  |  |
| When handing over the management and control of the completed works during construction, installation and commissioning from one organisation to another, it shall be ensured that the documentation related to the SSCs is verified for its completeness and accuracy, that all the non-compliances or unfinished works can be identified and resolved in a way that will not affect safety. | COM | Quality assurance program is summarized in DCD section 17. |
| Article 166 |  |  |
| The following shall be developed, introduced and provided before the commissioning:  1. Organisational documents for commissioning management;  2. Commissioning limits and conditions;  3. Operating procedures and maintenance, tests and surveillance instructions for SSCs important to safety;  4. Documents of the management system, including those for change control;  5. Emergency operating procedures and on-site emergency plan for the NPP;  6. Physical protection system and fire safety system;  7. Sufficient personnel with the required qualification and certification. | OR/NAS | All necessary procedures will be developed before the commissioning.  Standard AP1000 Operating procedures are already developed: General, Refueling, Abnormal Operating Procedures (AOPs) , Emergency Operating Procedures (EOPs) , Post-72 Hour Recovery Procedures, Alarm Response Procedures (ARPs), Maintenance, Test, Inspection, Surveillance Procedures (MTISs) including Severe Accident Mitigation Guidelines (SAMGs). These shall be used as input for Kozloduy Units Operating Procedures. |

### Section II: Commissioning Program

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 167 | | |
| The operating organisation shall develop and implement a commissioning programme covering all the operational states. The results of the programme implementation shall demonstrate compliance of the characteristics of SSCs important to safety, and the NPP process parameters with the design requirements and the provisions of the commissioning permit issued by the Chair of the Nuclear Regulatory Agency. | OR | Requirement for the Owner.  Standard AP1000 Operating procedures are already developed: General, Refueling, Abnormal Operating Procedures (AOPs) , Emergency Operating Procedures (EOPs) , Post-72 Hour Recovery Procedures, Alarm Response Procedures (ARPs), Maintenance, Test, Inspection, Surveillance Procedures (MTISs) including Severe Accident Mitigation Guidelines (SAMGs). These shall be used as input for Kozloduy Units Operating Procedures. |
| Article 168 | | |
| (1) The commissioning programme shall ensure that:  1. all the necessary tests to confirm the compliance of the constructed nuclear power plant with the design requirements are completed;  2. tests were performed in their logical sequence;  3. the "hold points" were identified in the commissioning process;  4. the operating personnel was trained and the instructions validated; | OR | Requirement for the Owner.  See assessment of Article 95. |
| (2) The tests conducted under the commissioning programme shall not lead to operational states and accident conditions that have not been analysed in the interim safety analysis report. | OR/COM-B | The initial test program is described in DCD chapter 14. Detailed commissioning programme will be specified more in detail during construction phase. |
| Article 169 | | |
| (1) The NPP commissioning shall be performed in sequential stages, for which separate programmes shall be developed. The implementation of each stage shall be preceded by an evaluation of the results from the previous stage and a confirmation that the objectives set and design requirements have been met. | OR/COM-B | The initial test program is described in DCD chapter 14. Commissioning schedule will be specified more in detail during construction phase.  See assessment of Article 95. |
| (2) The programme for each stage shall describe:  1. The sequence, timing and logical connections between the activities at the stage;  2. The initial and final status at the respective stage;  3. The organisation for implementation and the required personnel;  4. The preconditions for implementation of the tests;  5. The requirements on the technological preparation and provision of power sources and operating fluids;  6. The criteria for acceptance and an assessment of their fulfilment;  7. The conditions for transition to the next stage. | OR/COM-B | The initial test program is described in DCD chapter 14. Commissioning schedule will be specified more in detail during construction phase. |
| (3) The programmes for each stage shall contain a time schedule and a list of procedures to be followed during the tests. | OR/COM-B | The initial test program is described in DCD chapter 14. Commissioning schedule will be specified more in detail during construction phase. |
| Article 170 | | |  | Initial test program is described in DCD chapter 14. Commissioning schedule will be specified more in detail during construction phase. |
| (1) The tests shall be carried out in accordance with written procedures that shall have as a minimum requirements on:  1. Introduction and withdrawal of temporary modifications necessary to conduct the testing;  2. Verification that the prerequisites and the preconditions to conduct the tests are fulfilled;  3. Measurement equipment used and its calibration;  4. Limits and conditions to conduct the testing;  5. Test results recording means;  6. Acceptance criteria for the results and their allowable ranges;  7. Clear and unambiguous instructions on the test performance;  8. Clear rules to follow when the acceptance criteria are not met;  9. Plant recovery to normal state following the test performance. | OR/COM-B | The initial test program is described in DCD chapter 14. Written procedures will be specified during construction phase. |
| (2) The developing, approving, modification, distribution and storage of the test procedures and the reporting documents containing the results thereof shall be in compliance with the management system. | OR/COM-B | The initial test program is described in DCD chapter 14. Written procedures will be specified during construction phase. |
| Article 171 | | |
| The test results approval shall be arranged in a way that the following objectives are met:  1. The NPP behaviour has been compared with the design requirements;  2. Sufficient data on the revaluation of the design bases are ensured, in case the unit behaviour deviates from the expectations;  3. Demonstrate that the NPP as tested allows to proceed with the next stage of commissioning or with the next test. | COM-B | The initial test program is described in DCD chapter 14. Test program will be specified more in detail during construction phase. |
| Article 172 | | |
| (1) The commissioning activities shall be carried out in compliance with the commissioning programme, testing procedures, operation, maintenance, surveillance and inspections. | OR/COM-B | The initial test program is described in DCD chapter 14. Commissioning activities will be specified more in detail during construction phase. |
| (2) The applicability and quality of the operating procedures shall be confirmed (validation and verification) during the commissioning process. | OR/COM-B | The initial test program is described in DCD chapter 14. Commissioning activities will be specified more in detail during construction phase. |
| Article 173 | | |
| (1) Before the initial core loading with nuclear fuel: SSCs important to safety and required at this stage shall be tested and their availability shall be confirmed; tests to determine the characteristics of the reactor coolant pressure boundary shall be carried out; biological shielding effectiveness shall be tested; radiation monitoring shall be carried out at the premises, site, precautionary action zone and surveillance zone. | OR/CWO | The minimum conditions for initial fuel loading are specified in DCD 14.2.7.1 and will be specified more in detail during construction phase. |
| (2) Before reaching initial criticality of the reactor installation, functional tests of SSCs important to safety shall be carried out to confirm the fulfilment of the design functions and the compliance with the design characteristics. | OR/CWO | The minimum conditions before reaching initial criticality are specified in DCD 14.2.7.2 and will be specified more in detail during construction phase. |
| (3) The transition from one power level to another shall be performed after successful neutron physics test (experiments) of the reactor installation and completion of all construction and assembly works. | COM-B | Tests performed during power ascension program are described in DCD section 14.2.7.3 and will be specified more in detail during construction phase. |
| (4) Trial-testing operation shall be performed as a commissioning stage for evolutionary NPPs. | N/A or COM-B | Not applicable to AP1000 Design. However, this need to be discussed to understand its impact in the project. |
| Article 174 | | |
| A nuclear power plant unit, which is in a process of commissioning, shall be physically isolated from other units that are in operation or under construction at the same site. | COM-B | NPP shall be physically isolated from other units. |

## CHAPTER 8 – OPERATIONS

### Section I: Operational Safety Management

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 175 | | |
| (1) The management body of the operating organisation shall establish a document defining the safety policy which prioritises safety in all activities and shall demonstrate clear commitment to continuously improve safety and stimulate personnel’s critical attitude to the work performed in order to achieve best results. | OR | Requirement for the Owner. |
| (2) The personnel performing safety related activities shall be familiar with the Safety Policy to an extent ensuring clear understanding and application. Contractors shall be acquainted with the key aspects of the Safety Policy in order to understand and observe the requirements of the operating organisation. | OR | Requirement for the Owner. |
| Article 176 | | |
| (1) The Safety Policy shall provide for the issue of procedures on its application and monitoring of activities with impact on safety. | OR | Requirement for the Owner. |
| (2) The Safety Policy shall define clear-cut safety objectives and intentions which can be easily controlled and tracked by the management personnel. | OR | Requirement for the Owner. |
| (3) The Safety Policy shall stipulate continuous enhancement of nuclear safety by means of:  1. Continuous process of reassessment of the nuclear power plant safety taking into account the operating experience, safety assessments and analyses, and research and technological developments;  2. Timely implementation of feasible improvements;  3. Timely application of important new information which may be related to the nuclear power plant safety. | OR | Requirement for the Owner. |
| (4) The adequacy and status of implementation of the Safety Policy shall be assessed more frequently than the Periodic Safety Review. | OR | Requirement for the Owner. |
| Article 177 | | |
| (1) The nuclear power plant shall be operated safely, providing that:  1. Safety related decisions shall be made in a timely manner and preceded by the relevant research and consultations in order to consider all safety aspects;  2. The safety problems shall be subjected to safety analyses conducted by qualified personnel not involved in the operations;  3. Personnel shall be provided with the required technical means and work conditions in order to perform their activities in a safe manner;  4. Work performance shall be continuously monitored based on the relevant management processes in order to ensure sustaining the required safety level as well as its enhancement, if necessary;  5. Applicable operating experience, development of international safety standards, and new knowledge gained through research and development projects shall be continually analysed and used to improve the NPP as well as the activities involved in its operation;  6. The processes shall be managed using a documented management system covering all the activities, including contractors’ ones, that may impact the safe operation. | OR | Requirement for the Owner. |
| (2) Compliance with safety regulations as well as physical protection regulations shall meet the safety objectives as well as the physical protection objectives. Possible conflicts shall be solved based on cooperation between the safety officers and physical protection officers. | OR | Requirement for the Owner. |
| (3) Occupational safety provisions shall be integrated with the nuclear safety and radiation protection programmes in such a manner as to keep the safety risk as low as reasonably achievable. | OR | Requirement for the Owner. |
| Article 178 | | |
| (1) As part of the operation of a nuclear power plant, a system for continuous monitoring of safety and performance of activities shall be developed and implemented. Systematic self-assessment at all levels of the operating organisation shall be an integral part of this system. | OR | Requirement for the Owner. |
| (2) Monitoring and self-assessment shall determine the level of safety performance achieved as well as any indications of a degraded safety. | OR | Requirement for the Owner. |
| (3) The monitoring shall cover personnel behaviour and attitude towards safety as well as any breaches of the operational limits and conditions, operating procedures, regulatory requirements, and provisions of the operating licences. For the purpose of monitoring the condition of the NPP, implementation of activities, and personnel behaviour, the plant managers shall conduct systematic walkdowns. | OR | Requirement for the Owner. |
| (4) Relevant indicators of safety performance shall be developed and implemented enabling plant managers to detect and correct any weaknesses and non-conformances in safety management. | OR | Requirement for the Owner. |
| (5) Based on the monitoring and review of safety performance, corrective actions shall be identified and implemented, controlled and assessed. | OR | Requirement for the Owner. |
| Article 179 | | |
| (1) Periodic Safety Reviews shall assess the consequences of the cumulative ageing effects, modifications and requalification of SSCs, operating experience, current safety standards and research and development achievements, changed features of the NPP site, and organisational and managerial problems. Periodic reviews shall focus on ensuring high level of safety throughout the operating life of the NPP. | OR | Requirement for the Owner. |
| (2) The review scope shall cover the safety factors under Article 89 which shall be assessed using deterministic methods. Within the meaning of Article 80 (1), probabilistic analyses may be used in the summarised safety assessment mostly to determine the contribution of the detected facts to the common safety level. | OR | Requirement for the Owner. |
| (3) Based on the results, all the corrective actions and feasible modifications shall be implemented to achieve the safety level prescribed in the current safety standards. | OR | Requirement for the Owner. |
| Article 180 | | |
| (1) During normal operation, all physical barriers shall be effective and all levels of defence shall be available. In case of a failure of a physical barrier or unavailability of a level of defence, the reactor shall be brought to a safe shutdown condition. | OR | Requirement for the Owner. |
| (2) A failure of a physical barrier or unavailability of a level of defence at all operational states shall be justified in the design as well as in the safety assessment of the NPP. | OR | Requirement for the Owner. |
| Article 181 | | |
| (1) To maintain the availability of the levels of defence, the NPP operation shall comply with the operational limits and conditions. | OR | Requirement for the Owner. Technical specifications are presented in DCD section 16, and will be revised during construction and commissioning, if necessary. |
| (2) The operational limits and conditions shall be defined and justified on the basis of design, safety analyses and commissioning tests, and shall be reviewed periodically and as necessary to reflect the operating experience, modifications of SSCs important to safety, latest safety analyses, and research and technological developments. | COM  OR | Technical specifications are presented in DCD section 16, and will be revised during construction and commissioning, if necessary.  Updates during power operation are in the responsibility of the Owner. |
| (3) Changes of the operational limits and conditions shall be justified based on analyses of the safety margins and independent review of those analyses. | COM  OR | Technical specifications are presented in DCD section 16, and will be revised during construction and commissioning, if necessary.  Updates during power operation are in the responsibility of the Owner. |
| Article 182 | | |
| (1) The operational limits and conditions shall cover all the normal operation states, including power operation, subcritical reactor, core refuelling, and all the transients between those states, operational states, or temporary conditions resulting from maintenance works and testing, and shall include as a minimum:  1. Safety margins;  2. Safety system actuation parameters;  3. Operational limits and conditions;  4. Tests, inspections, surveillance, and on-line monitoring of SSCs important to safety;  5. Minimum number of shift personnel for the operational states, including the certified and qualified MCR operators;  6. Actions to be taken in case of deviations from the operating limits and conditions. | COM | Technical specifications are presented in DCD section 16, and will be revised during construction and commissioning, if necessary. |
| (2) In order to prevent any undesirable frequent actuation of the safety system, adequate margins shall be ensured between the operating limits and the safety system actuation parameters. | COM | Technical specifications are presented in DCD section 16 with adequate margins, and will be revised during construction and commissioning, if necessary. |
| (3) A conservative approach shall be used to define the safety limits, taking into account the uncertainties of the safety analyses. | COM | Safety limits are defined in DCD section 16 with the consideration of the results of the safety analyses, and will be revised during construction and commissioning, if necessary. |
| (4) The operating limits and conditions shall cover operating parameter limits, minimum number of operable SSCs (in service or standby) for each normal operation state, the actions to be taken in case of a deviation from the operating limits, and time for execution of those actions. | COM | Technical specifications are presented in DCD section 16 with the consideration of operating parameter limits, minimum number of operable SSCs and actions with execution time in case of a deviation. Technical specifications will be revised during construction and commissioning, if necessary. |
| (5) If the conditions for operability of the SSCs important to safety can not be met, the actions and time to bring the power unit to a safe and stable state shall be identified. | COM | Technical specifications are presented in DCD section 16 with the consideration of actions and time to bring the NPP to safe and stable state. Technical specifications will be revised during construction and commissioning, if necessary. |
| Article 183 |  |  |
| (1) In case the operators are unable to verify that the power unit is operated within the operating limits, or the unit behaviour is unexpected, immediate actions shall be taken to bring it to a safe and stable state. | OR | Requirement for the Owner. |
| (2) The power unit shall not be restarted after an unplanned shutdown unless it is demonstrated that this can be executed safely. | OR | Requirement for the Owner. |
| Article 184 | | |
| (1) The surveillance programme shall cover monitoring of compliance with the operating limits and conditions, including the trends within the established margins, in order to detect any deviations from the design targets. | COM | Surveillance requirements are presented in DCD section 16. Technical specifications will be revised during construction and commissioning, if necessary. |
| (2) In case of noncompliance with the operating limits and conditions, immediate actions shall be taken to restore compliance with the requirements. In order to prevent recurrence of such noncompliances, corrective actions shall be implemented. | OR | Requirement for the Owner. |
| (3) The cases when the actions taken to correct deviations from the operating limits and conditions differ from the prescribed ones, including the cases when the established times for implementation of those actions are exceeded, shall be considered noncompliances with the operating limits and conditions. | OR | Requirement for the Owner. |
| Article 185 | | |
| The operating limits and conditions collected in a single document (Technical Specifications for Operation) shall be easily accessible to the MCR personnel, who shall be knowledgeable of them and their technical basis. The management of the operating organisation shall be well aware of their significance for safety. | COM  OR | Technical specifications are easily accessible to the MCR personnel.  Training of MCR personnel and management of operating organization is the responsibility of the Owner. DCD section 18.10 presents designer’s input to the training program. |
| Article 186 | | |
| (1) Activities with an impact on safety shall be analysed and monitored to ensure that the radiological risk remains as low as reasonably achievable when those activities are performed. | OR | Requirement for the Owner. |
| (2) All operators’ actions shall be assessed against their potential risk. The level of assessment and monitoring of the activities shall depend on their significance for safety.  Testing of SSCs important to safety, special operational states, or experiments which are not included in the Technical Specifications for operation or in the operating procedures shall be assessed against their impact on safety and carried out in compliance with special programmes and procedures following a positive statement issued by the Bulgarian Nuclear Regulatory Agency. | COM  OR | Implementation of task analysis is part of the HFE program, described in DCD section 18.5.  Testing and experiments during NPP operation is in the responsibility of the Owner. |
| Article 187 | | |
| (1) The nuclear power plant shall be managed by competent managers who are familiar with the safety assurance principles, specifics of the technological process, and related risks. All the activities with an impact on safety shall be performed by appropriately qualified and experienced personnel. | OR | Requirement for the Owner. |
| (2) The NPP operational state and the changes therein shall be monitored and controlled by certified and qualified operators as stipulated in the Safe Use of Nuclear Energy Act. | OR | Requirement for the Owner. |
| (3) At least two operators shall be available at the MCR during plant operation and their certificates of competency shall be issued by the Chair of the Nuclear Regulatory Agency. | OR | Requirement for the Owner. |
| (4) The duties and authority of the operators and safety officers shall be defined in job specifications and job descriptions for each job position. | OR | Requirement for the Owner. |
| Article 188 | | |
| (1) The shift personnel shall operate the NPP in compliance with written operating procedures and instructions. Strict observance of procedures and instructions shall be an essential element of the NPP Safety Policy. | OR | Operating procedures and instructions are prepared during the construction phase. Standard AP1000 Operating procedures are already developed: General, Refueling, Abnormal Operating Procedures (AOPs) , Emergency Operating Procedures (EOPs) , Post-72 Hour Recovery Procedures, Alarm Response Procedures (ARPs), Maintenance, Test, Inspection, Surveillance Procedures (MTISs) including Severe Accident Mitigation Guidelines (SAMGs). These shall be used as input for Kozloduy Units Operating Procedures.  Observance of the procedures and instructions is in the responsibility of the Owner. |
| (2) The level of detail of procedures and instructions shall be based on their intended purpose. The guidance shall be clear and concise, verified, and validated. | OR/COM-B | Operating procedures and instructions are prepared during the construction phase. Standard AP1000 Procedures will be used as input. |
| (3) Procedures, instructions, and aids shall be clearly identified, discernible in respect of intended function, and readily accessible at the MCR and other control rooms, if necessary. | OR/COM-B | Operating procedures and instructions are prepared during the construction phase. Standard AP1000 Procedures will be used as input. |
| Article 189 | | |
| (1) The operating procedures and instructions for normal operation shall be prepared based on the design and engineering documentation, operating limits and conditions, and results of plant commissioning. | OR/COM-B | Operating procedures and instructions are prepared during the construction phase. Standard AP1000 Procedures will be used as input. |
| (2) Operators’ emergency response actions for all the operational states shall be stipulated in Emergency Procedures and Severe Accident Management Guidelines (SAMGs). | OR/COM-B | Emergency procedures and SAMGs are prepared during construction phase. Standard AP1000 Procedures will be used as input. |
| Article 190 | | |
| (1) The Emergency Procedures shall cover the design basis accidents and scenarios where a significant fuel damage at the core or at the spent fuel pool can be prevented. The Emergency Procedures shall be symptom-based (SB EOPs) and compatible with the Alarm Instructions and SAMGs. | OR/COM-B | Emergency procedures are prepared during construction phase. See APP-GW-G0R-010 [31] |
| (2) The Design Basis Accident Emergency Procedures shall prescribe how to bring the plant to a stable safe condition, while the Emergency Procedures for the scenarios where a significant nuclear fuel damage can be prevented shall prescribe how to restore or compensate for lost safety functions as well as how to prevent nuclear fuel damage at the core or at the spent fuel pool (SFP). | OR/COM-B | Emergency procedures are prepared during construction phase. Standard AP1000 Procedures will be used as input. See APP-GW-G0R-010 [31] |
| (3) The set of SB EOPs shall include:  1. State diagnostic procedures;  2. Procedures for optimal recovery in the event of transients and design basis accidents;  3. Condition monitoring procedures and procedures for restoration of safety functions, such as subcriticality, core cooling, residual heat removal, coolant inventory, integrity of the reactor coolant pressure boundary and containment integrity;  4. Procedures for transition to severe accident management. | OR/COM-B | Emergency procedures are prepared during construction phase. Standard AP1000 Procedures will be used as input. See APP-GW-G0R-010 [31] |
| (4) For the preparation of SB EOPs, their format, structure, and contents shall be specified in a way that:  1. Gives precise, clear, and adequate guidance for the personnel to perform the prescribed actions, including when a transition to other procedures, instructions, and guidelines is required, considering only the operation of the equipment and instruments qualified for the relevant work environment;  2. It is easy to distinguish them from the Normal Operation Procedures and it is convenient to use them;  3. They include instructions for monitoring of specific process parameters (symptoms), for monitoring of automated system responses, fundamental operators’ actions for immediate execution and the anticipated result of them, as well as alternative operators’ actions in case of failure of the fundamental ones;  4. The supplementary background information that aids the operators in observing the procedures is clearly discriminated. | OR/COM | Emergency procedures are prepared during construction phase. Standard AP1000 Procedures will be used as input. See APP-GW-G0R-010 [31] |
| Article 191 | | |
| (1) The Severe Accident Management Guidelines shall result in mitigation of consequences of severe accidents when the personnel actions, including the actions prescribed in the SB EOPs, have not been successful in preventing core damage or fuel damage at the SFP. | OR/COM-B | SAMGs are prepared during construction phase. Standard AP1000 SAMGs will be used as input. See APP-GW-G0R-010 [31] |
| (2) The Severe Accident Management Guidelines and SB EOPs shall:  1. Provide for the management of accidents impacting both the reactor and spent fuel pool and consider the possible interaction between the reactor and SFP;  2. Consider the capabilities for one of one powerunit to support another power unit on the NPP site without compromising its own safety;  3. Ensure their implementation, even when all the on-site nuclear facilities are in accident conditions, and take into account the dependencies among the systems and common resources;  4. Consider the expected conditions on the NPP site, including the radiological situation resulting from the accidents which they are intended for as well as the initiating event or external hazard that may have caused it. | OR/COM-B | SAMGs and EOPs are prepared during construction phase. See APP-GW-G0R-010 [31] |
| Article 192 | | |
| (1) Severe Accident Management Guidelines shall be based on strategies for management of the scenarios resulting from the analysis of the weaknesses and capabilities of the nuclear power unit in the event of a severe accident, and the possible measures for management including for containment protection. The SAMGs shall consider as a priority the operation of the equipment and instruments qualified for the relevant conditions. | OR/COM-B | SAMGs are prepared during construction phase. See APP-GW-G0R-010 [31] |
| (2) For the preparation of SAMGs and SB EOPs, unit-specific data shall be used. The effectiveness of the operators’ actions shall be analytically validated using verified computer codes and unit-specific calculation models. The results of the analysis shall be documented and used as a technical basis for the procedures. | OR/COM-B | SAMGs and EOPs are prepared during construction phase. See APP-GW-G0R-010 [31] |
| (3) The emergency procedures and guidelines shall be verified and validated by an independent team of experts according to established internal rules (programmes) in the form they are used. The practical capability to execute the operators’ actions shall be validated using simulator tools. | OR/EP | Owner Requirement. See APP-GW-G0R-010 [31] |
| (4) The up-to-dateness of the emergency procedures and guidelines shall be verified by the operating organisation periodically. | OR | Requirement for the Owner. |
| Article 193 | | |
| (1) Throughout the operation of the NPP, a configuration management process shall be developed and implemented to ensure correspondence between the design requirements, physical configuration of SSCs important to safety, and operating documents. | COM  OR | During design, construction and commissioning, a quality assurance program is maintained to ensure the quality of the products.  During operation, configuration management process is in the responsibility of the Owner. |
| (2) The organisational measures in respect of configuration management shall ensure that the modifications of the NPP and SSCs important to safety are identified, designed, assessed, implemented, and documented. | COM  OR | During design, construction and commissioning, a quality assurance program is maintained to ensure the quality of the products.  During operation, configuration management process is in the responsibility of the Owner. |
| (3) The appropriate organisational measures shall be planned for the NPP configuration changes resulting from maintenance, tests, repairs, and modernisation of the NPP. | COM  OR | During design, construction and commissioning, a quality assurance program is maintained to ensure the quality of the products.  During operation, configuration management process is in the responsibility of the Owner. |
| Article 194 | | |
| Temporary and permanent modifications of SSCs important to safety shall be planned, controlled, and implemented so as not to compromise the safe operation of the plant. Changes, including the ones related to the organisational structure, operating limits and conditions, procedures and instructions, methods and computer codes for safety assessment, shall be categorised based on a graded approach with appropriate criteria in respect of their safety significance. | COM  OR | During design, construction and commissioning, quality assurance program is maintained to ensure the quality of the products due to modifications of the plant.  During operation, configuration management process is in the responsibility of the Owner. |
| Article 195 | | |
| (1) When modifying SSCs important to safety, the following sequence of steps shall be performed:  1. Identification of the causes and justification of the need for modification;  2. Identification of the requirements for design and safety assessment scope and methods;  3. design and justification of safety, manufacturing, procurement, installation, and testing;  4. Documents changes and personnel training;  5. Implementation of the modification. | COM  OR | During design, construction and commissioning, quality assurance program is maintained to ensure the quality of the products due to modifications of the plant.  During operation, configuration management process is in the responsibility of the Owner. |
| (2) The initial safety assessment shall assess and justify the category of the modification proposed. A detailed and comprehensive safety assessment shall be conducted unless the initial assessment has demonstrated that the scope of this assessment can be reduced in order to demonstrate that all safety aspects have been considered and the applicable safety requirements met. The scope, safety level conclusions, and consequences of the modifications proposed shall be assessed by the personnel who have not taken part initially in their designing or implementation. | COM  OR | Design changes during design phase, construction and commissioning are handled by quality assurance program, see DCD section 17.  During operation, safety assessment process is in the responsibility of the Owner. |
| (3) The implementation and tests of SSCs modifications, their impact on procedures and personnel training, including at the full scope simulator, shall be conducted in compliance with the Management System processes and documents. | COM  OR | Design changes during design phase, construction and commissioning are handled by quality assurance program, see DCD section 17.  During operation, implementation of necessary tests is in the responsibility of the Owner. |
| (4) Prior to commissioning of modifications, the personnel shall be trained on their servicing and operation, and all the relevant operating procedures shall be modified or updated. | COM  OR | Design changes during design phase, construction and commissioning are handled by quality assurance program, see DCD section 17.  During operation, necessary training is in the responsibility of the Owner. |
| Article 196 | | |
| (1) Temporary modifications of safety related SSCs shall be managed in accordance with specific instructions. All temporary modifications shall be tagged in the field and marked on the alarm panels and controls. The operators shall be aware of those modifications and their effect on the operation of the plant. | COM  OR | Temporary design changes during commissioning are handled by quality assurance program, see DCD section 17.  During operation, instructions for temporary modifications is in the responsibility of the Owner. |
| (2) The number and duration of the temporary modifications shall be limited to a minimum. The need for the temporary modifications to remain effective shall be assessed periodically. | COM  OR | Temporary design changes during commissioning are minimized.  Temporary design changes during operation, is in the responsibility of the Owner. |
| Article 197 | | |
| (1) Throughout the operation, a programme shall be drawn up and systematically applied to collect, analyse, and document internal and external operating experience as well as the operating events occurring at the plant. | OR | Requirement for the Owner. |
| (2) Based on the assessment of the plant operating experience, the latent weaknesses in respect of safety, potential preconditions and possible trends towards poor performance of activities impacting safety or reducing the safety margins shall be identified. Significant findings and trends shall be reported to the plant management. | OR | Requirement for the Owner. |
| (3) For implementation of the programme specified in paragraph 1, for dissemination of the results important to safety, and for identification of recommendations for improvements, personnel who are adequately trained, provided with resources, and supported by the plant management shall be assigned. | OR | Requirement for the Owner. |
| (4) To prevent recurrence and counteract events compromising safety, the recommendations for improvement shall be implemented, timely and adequate corrective actions shall be taken, and the best practices shall be considered. | OR | Requirement for the Owner. |
| (5) The information related to the operating experience and safety shall be organised, documented, and stored in a manner facilitating its accessibility, screening, and assessment by the personnel assigned for that purpose. | OR | Requirement for the Owner. |
| Article 198 | | |
| (1) Safety significant operating events shall be reported in accordance with established procedures and criteria. Plant personnel shall report deviations from normal operation and shall be encouraged to report safety significant near misses. | OR | Requirement for the Owner. |
| (2) In the event of safety significant failures or deviations from normal operation, consultation shall be ensured on the required corrective actions from the manufacturer of the SSCs, from the designer, or from the plant R&D manager. | OR | Requirement for the Owner. |
| Article 199 | | |
| Information based on the operating experience shall be disseminated to the relevant personnel, shared with the interested national and international organisations, and used in the training of the personnel performing activities with impact on safety. | OR | Requirement for the Owner. |
| Article 200 |  |  |
| Periodic reviews of the operating experience feedback efficiency, based on specific indicators or criteria, shall be conducted by the operating organisation as part of the self-assessment process or by an independent team. | OR | Requirement for the Owner. |
| Article 201 | | |
| (1) Throughout the operation of the NPP, specifications and procedures shall be prepared for procurement, verification, receipt, accountability and control, loading, use, refuelling, and testing of nuclear fuel and core components. | OR | Requirement for the Owner. |
| (2) Only nuclear fuel manufactured in accordance with the established specifications and design criteria for the nuclear fuel and its enrichment shall be loaded into the core. | OR | Requirement for the Owner. |
| (3) The use of a new type of nuclear fuel shall be deemed to be a modification significantly changing the plant configuration and shall be preceded by a detailed and comprehensive safety assessment. | OR | Requirement for the Owner. |
| Article 202 | | |
| (1) The decisions, planning, assessment, execution, and supervision of all operations or modifications involving nuclear fuel and having a potential impact on the reactivity control shall be undertaken in compliance with the reactivity control programme, approved procedures, and operating limits and conditions for the nuclear fuel. | OR | Requirement for the Owner. |
| (2) Regarding core monitoring, a programme shall be drawn up and implemented to ensure that:  1. The core parameters have been measured, trends have been analysed and assessed in order to detect defects in the nuclear fuel;  2. The actual state of the core complies with the design requirements;  3. The values of the basic operating parameters are recorded and stored in a logical, consistent, and easy to use manner. | OR/COM | Requirement for the Owner.  The reactor design contains a core power distribution measurement system designated as the incore instrumentation system (IIS). The IIS incorporates incore instrument thimble assemblies (IITAs). Each IITA contains multiple self-powered neutron detectors. The detectors are sequentially increasing in length and distributed axially and radially within the reactor core to provide continuous measurements of signals directly proportional to the neutron flux present around each IITA. The measured signals are processed by the signal processing system (SPS) cabinets and application servers for use by the core power monitoring software (BEACON™ Core Monitoring System). The IITAs also contain thermocouples to measure core exit temperature for post-accident monitoring. The best-estimate analyzer for core operations–nuclear (BEACON) system uses the fixed incore detector signals in conjunction with analytically derived constants and other plant sensor signals to continuously generate full three-dimensional indications of nuclear power distribution in the reactor core, and to determine if the reactor power distribution is currently within the predefined operating limits when the reactor is operating above 20% of rated thermal power.  In the unlikely event that the online monitoring system is out of service, power distribution controls based on bounding, pre-calculated analyses are also provided to the operator. As a result, the online monitoring system is not a required element of reactor operation. Signals are available to the operator from the ex-core ion chambers, which are long ion chambers outside the reactor vessel that run parallel to the axis of the core. Separate signals are taken by each ion chamber. The ion chamber signals are processed and calibrated against incore measurements and the difference in indicated power between the core top and bottom halves is derived for each of four channels of ex-core detectors. |
| Article 203 | | |
| (1) Operations influencing reactivity shall be executed with consideration and care to ensure the reactor remains within the operating limits and conditions, reaching the expected response of the reactor installation. | OR | Requirement for the Owner. |
| (2) The operating procedures concerning reactor start-up, power operation, shutdown, and core refuelling shall include safeguards and controls necessary to ensure nuclear fuel integrity and compliance with the operating limits and conditions throughout the entire period of nuclear fuel operation. | OR/COM-B | Operating procedures and instructions are prepared during construction phase. Standard AP1000 Procedures will be used as input. See APP-GW-G0R-010 [31]. |
| (3) Procedures governing the operations involving nuclear fuel and core components shall ensure controlled handling of fresh and irradiated nuclear fuel, adequate storage, transfer or transport preparation. A person having the required experience, knowledge, and qualification shall be assigned in charge of the supervision and conduct of the operations involving nuclear fuel. | OR/ COM-B | Operating procedures and instructions are prepared during construction phase. Standard AP1000 Procedures will be used as input. See APP-GW-G0R-010 [31].  It is Owner’s requirement to have a person with sufficient experience and knowledge to lead supervision and conduct of operations. |
| Article 204 | | |
| (1) Outage planning shall be a continuous process, focused on improvements, accounting for completed, forthcoming, and future major maintenance activities. | OR | Requirement for the Owner. |
| (2) The process of planning and performing outage activities shall consider and prioritise the safety factors. Special attention shall be paid to the reactivity control, residual heat removal, nuclear fuel handling, and ensuring reactor pressure boundary integrity and containment integrity. Plant configuration management in this operational state shall comply with the operating limits and conditions. | OR | Requirement for the Owner. |
| (3) Programmes and procedures shall be issued to enable outage management and provide the required resources for ensuring safety. | OR | Requirement for the Owner. |
| (4) Tasks, responsibilities, authority, and lines of communication of the teams and persons taking part in the preparation, implementation, and assessment of the outage schedules and activities shall be stipulated in administrative procedures and observed by the plant and contractors’ personnel. | OR | Requirement for the Owner. |
| (5) Outage programmes and procedures shall account for the optimisation of the radiation protection and industrial safety of the personnel, minimisation of the generated radioactive waste, and control of chemical hazards. | OR | Requirement for the Owner. |
| (6) Upon completion of each outage, a detailed review of the activities shall be conducted to document the lessons learned. | OR | Requirement for the Owner. |
| Article 205 | | |
| During plant operation, fire safety measures identified in the fire hazard analysis shall be taken. Those measures include requirements for management of the activities impacting fire safety – maintenance, combustible material management, personnel training, testing and emergency exercises, changes in location and configuration of the fire suppression systems, fire detection, ventilation systems, power supply systems, fire safety control systems and process control systems. | OR | Requirement for the Owner. |
| Article 206 | | |
| (1) In order to prevent internal fires, procedures shall be established for the management and minimisation of combustible materials and potential ignition sources that may affect SSCs important to safety. Those procedures shall ensure the operability of fire fighting technical means through inspections, maintenance, and testing of the fire barriers, fire suppression systems, fire detection and alarm systems, and portable fire fighting equipment. | OR | Requirement for the Owner. |
| (2) Responsibilities and actions of the personnel in case of fire shall be stipulated in a fire fighting strategy and emergency procedures that are to be learnt in the course of emergency exercises. This strategy shall cover each area where an internal fire may affect SSCs important to safety as well as the radioactive material protection. | COM-B  OR | EOPs are prepared during construction phase.  Otherwise, this requirement is for the Owner. |
| Article 207 | | |
| (1) When national or local fire brigades are involved in the fire fighting, coordination shall be established between the plant personnel and those bodies who shall be familiarised with the risks at the NPP. | OR | Requirement for the Owner. |
| (2) When plant personnel take part in fire fighting activities, their organisation and number, competence certification and training requirements shall be documented and verified by an officer competent in fire protection. | OR | Requirement for the Owner. |
| (3) Joint emergency exercises shall be conducted periodically to assess fire fighting performance. | OR | Requirement for the Owner. |
| Article 208 | | |
| In case the operating organisation intends to operate the plant beyond the established design life, a large-scale long term operation programme shall be drawn up and implemented, covering the following:  1. Preliminary conditions, including licensing basis, implemented measures for enhancement and verification of the safety level, and existing operating programmes;  2. Identification of SSCs to be covered by the Programme;  3. Categorisation of SSCs in respect of ageing and degradation processes and selection of a strategy for extension of their design life if necessary;  4. Conducting of new safety analyses based on time-limited assumptions and initial conditions;  5. Preparatory plan for long term operation. | OR | Requirement for the Owner. |

### Section II: Conduct of Operations

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 209 | | |
| The administrative unit in charge of the plant operations shall perform the following tasks, functions, and duties:  1. Planning of all the activities related to the plant operations while preparing an integrated operations programme together with the other administrative units;  2. Planning of human resources and operators’ career development;  3. Direct operation of the plant based on monitoring and control of the systems in compliance with the established rules, operating and administrative procedures, and operating limits and conditions;  4. Supervision and control over the operators’ actions by the shift supervisor;  5. Organisation of surveillance of the core refuelling activity and outage;  6. Development of operating instructions and procedures and coordination of their preparation to ensure safe and reliable operation of the SSCs;  7. Coordination of the preparation and implementation of programmes and policies for safe operation;  8. Participation in the preparation of programmes for surveillance of SSCs important to safety and coordination of their implementation;  9. Development and performance of the operations management processes which provide operators with information about the activities being carried out and ensure maintaining of the plant configuration;  10. Configuration management based on exact implementation of the changes in the plant status required for the conduct of maintenance, modifications, and tests;  11. Detection of failures, defects, and shortcomings of SSCs in order to plan and effectively perform the maintenance activities;  12. Support of outages by assigning operators for the preparation of the schedule of activities, testing, identification and monitoring of the operating condition of components and systems, and return of the systems to service;  13. Preparation and implementation of procedures for prevention of unauthorised access to or interference with SSCs important to safety;  14. Identification of training needs and participation in the development of training programmes, supervision of training sessions, and assessment of training programmes;  15. Verification of the good housekeeping of rooms, SSCs, and the material condition of the plant areas the organisational unit is in charge of;  16. Identification of operating objectives and intentions which shall be in line with the common plant objectives and intentions;  17. Reporting and participation in the investigation of all operating events and deviations, including near-misses and low-level events, as well as in the identification of measures to reduce the potential of their recurrence;  18. Registration, assessment, and documentation of the safety significant internal and external operating experience and dissemination of information about it to the operators. | OR | Requirement for the Owner. |
| Article 210 | | |
| (1) During all operational states and accident conditions and at all times, the required number of qualified operators shall be ensured. | OR | Requirement for the Owner. |
| (2) The number and composition of operators’ shifts shall reflect the periodic training, assignments, and level of automation of the technological processes as well as the provision of diversity and competence redundancy within the shift. | OR | Requirement for the Owner. |
| (3) Interactions between the operators during the shift, conduct of operations, channels of communication and execution of commands, shift turnover, and relations with the other administrative units shall be stipulated in a procedure for the operational interactions. | OR | Requirement for the Owner. |
| Article 211 | | |
| (1) Habitability and good working conditions (lighting, noise, radiation level, temperature, means of communication) shall be maintained in the MCR and SCR during all operational states and accident conditions. | CWO | AP1000 MCR Remote Shutdown and Technical Support Center Capabilities:  **Main Control Room (MCR):**  The main control room emergency habitability system (VES) provides a supply of breathable air for the main control room (MCR) occupants and maintains the MCR at a positive pressure with respect to the surrounding areas whenever ac power is not available to operate the nuclear island nonradioactive ventilation system (VBS) or high radioactivity is detected in the MCR air supply.  The temperature and pressure in the MCR are maintained so that the combination of initial MCR environment conditions, minimized MCR equipment heat sources, MCR isolation, VES-supplied air, VES filtration, and MCR in leakage limitations adequately support the allowable number of MCR inhabitants for 72 hours after an accident. After 72 hours, the licensing and design basis is that VBS functionality is restored and that VBS fully supports MCR habitability.  VES is a passive safety system, It passively provides air form compressed air tanks, maintaining MCR overpressure and air filtration. MCR heat removal counts on passive heat sinks (structures and equipment inside the MCR envelop that absorb heat).  During Normal Operation Nuclear Island Nonradioactive Ventilation System (VBS) will provide the HVAC and control room habitability, supplying the MCR envelope. It will also serve other non-radioactive areas in the nuclear island that include Class 1E and non-1E electrical equipment rooms, remote shutdown workstation HVAC equipment rooms in the Auxiliary Building; Control Support Area/Technical Support Center (CSA/TSC) area in the Annex Building; and Passive Containment Cooling System (PCS) valve room in the Shield Building..  VBS shall:  • Provide isolation of the MCR envelope from the surrounding areas and outside environment during and following a design basis accident.  • Provide radiological monitoring of MCR supply air airborne process streams and initiation signals to the Protection and Safety Monitoring System (PMS) for actuation of the Main Control Room Emergency Habitability System (VES).  • After 72 hours after and accidental condition this system functionality is to be restored and provide MCR Habitability.  • Provide protection of MCR and/or CSA areas from infiltration of smoke from an external source.  • Provide smoke removal capability for the MCR envelope, CSA area and Class 1E electrical equipment rooms from an internal source.  **Remote Shutdown Workstation (RSW):**  AP1000 standard design includes remote shutdown capability is provided.  The Remote Shutdown Workstation (RSW) contains the indications and controls that allow an operator to achieve and maintain safe shutdown of the plant following an event when the MCR is unavailable. The RSW is not normally powered and requires control to be manually transferred from MCR if there is an event that requires evacuation of the MRC. Additional non-safety-related indications and controls are provided. As with the MCR, the RSW requires no ac power sources for its operation. It is mainly envisaged if MCR has to be evacuated due to a fire event.  Additionally, a secondary diverse actuation is located in a diverse spatially separated location (not in the same zone of the plant) to actuate key safety functions such as ADS Stage 4 actuation, IRWST injection and containment recirculation actuation. The secondary DAS panel is powered by an independent local battery. The secondary DAS panel is located sufficiently far from the Main Control Room (MCR) and Remote Shutdown Workstation), its location has been selected as to provide additional protection so that it is very unlikely that it could be affected by internal events such as fire, internal flooding, or external events such as flooding (thus providing additional protection from these events).  **Technical Support Center**  The mission of the technical support center (TSC) is to provide an area and resources for use by personnel providing plant management and technical support to the plant operating staff during emergency evolutions. The TSC relieves the reactor operators of peripheral duties and communications not directly related to reactor system manipulations and prevents congestion in the control room. The TSC is located in the control support area (CSA) of the Annex Building.  Communications needs are established for the staff within the TSC, and between the TSC and the plant (including the main control room and operational support center), the emergency operations facility, the Licensee, the outside authorities and the public.  The design includes adequate shielding as discussed in Chapter 12. Adequate space, resources and access is provided for maintenance, emergency equipment and storage. Consistent with NUREG 0737, the technical support center is nonsafety-related and is not required to be available after a safe shutdown earthquake.  The size of the TSC complies with the size requirements of NUREG-0696, “Functional Criteria For Emergency Response Facilities.”  The TSC complies with the habitability requirements of NUREG-0737, Supplement 1; “Requirements for Emergency Response Capability” when electrical power is available.  Should habitability be challenged within the TSC due to lack of cooling or a high radiation level resulting from a beyond-design-basis accident, the plant management function of the TSC is transferred to the main control room. |
| (2) The Emergency Response Centre, SCR, and all local control panels shall be kept operable, easily accessible and free of unnecessary materials, provided with the required documents and means of communication, and periodically inspected. | COM  OR | Emergency response center, remote shutdown station and all local control panels are easily accessible with the necessary communication means.  The Owner shall ensure that periodic inspections are performed to ensure operability and that they are free of unnecessary material. |
| (3) The MCR and SCR ventilation systems along with their filter modules shall be subject to periodic performance tests to ensure their compliance with the design characteristics and clean-up factors. | OR | Requirement for the Owner. |
| Article 212 | | |
| (1) Throughout the operation of an NPP, alarm procedures shall be prepared and implemented to stipulate operators’ actions in the event of alarm signals at the control panels and displays of the MCR information systems. Unexpected alarm signals shall be announced and documented. All alarm signals shall be treated as correct and valid unless they have been verified to be spurious based on assessment against other indications. | OR | Requirement for the Owner. Standard AP1000 Operating procedures are already developed including Abnormal Operating Procedures (AOPs) , Emergency Operating Procedures (EOPs) , and Alarm Response Procedures (ARPs). These shall be used as input for Kozloduy Units Operating Procedures. |
| (2) The information about the status of the alarm signals and their causes shall be available to the MCR operators. | OR/COM | Requirement for the Owner. |
| (3) Unavailability of alarm signals, both due to failure or deliberately taking out of service, shall be documented and the number of such cases shall be minimised. | OR | Requirement for the Owner. |
| (4) To determine whether the affected systems and components comply with the operating limits and conditions as well as to monitor the process parameters, the MCR operators shall be provided with alternative means. | OR | Requirement for the Owner. |
| (5) In the event of a transient, abnormal operation, or other situation involving multiple alarm signals, a detailed analysis shall be conducted to determine the unexpected or irrelevant alarm signals. | OR | Requirement for the Owner. |
| (6) When executing an emergency procedure, the MCR operators shall place a higher priority on the assessment of safety functions performance than on the assessment of the alarm signal status. | OR | Requirement for the Owner. Response will we performed by procedure.  Operating procedures and instructions are prepared during the construction phase. Standard AP1000 Operating procedures are already developed: General, Refueling, Abnormal Operating Procedures (AOPs) , Emergency Operating Procedures (EOPs) , Post-72 Hour Recovery Procedures, Alarm Response Procedures (ARPs), Maintenance, Test, Inspection, Surveillance Procedures (MTISs) including Severe Accident Mitigation Guidelines (SAMGs). These shall be used as input for Kozloduy Units Operating Procedures. |
| Article 213 | | |
| (1) To maintain water chemistry within the established margins, limit the ingress of chemical contaminants, and limit the radiological factors during the commissioning and operation of the plant, a programme for water chemistry and radiochemistry control shall be implemented. | COM-B | Water chemistry program is prepared during construction phase. It will be based on AP1000 standard Chemistry Manual, procedures, and specifications. |
| (2) This programme shall cover monitoring and data processing systems which, along with the laboratory analyses, shall provide for the measurement and recording of chemical and radiochemical parameters. | COM-B | The chemistry program shall be prepared during construction phase. It will be based on AP1000 standard Chemistry Manual, procedures, and specifications. |
| (3) The operators shall be able to correctly understand the chemical parameters, identify states deviating from the operating limits and conditions, detect adverse trends related to inadequate water chemistry, and take timely corrective actions when necessary. | OR | Requirement for the Owner. |
| (4) The data from the radiochemical analyses, which are representative of the integrity of the fuel rod cladding, shall be systematically monitored and analysed in order to assess the trends during all operational states. | OR | Requirement for the Owner. |
| (5) The use of chemical reagents shall be strictly monitored, including reagents brought to the plant by contractors. Appropriate engineering and organisational measures shall be in place when using chemical substances and reagents to prevent harmful effects or degradation of SSCs important to safety. | OR | Requirement for the Owner. |
| Article 214 | | |
| (1) During the operation of the power plant, good working conditions shall be maintained at all the working areas. The rooms, systems, and components shall be well maintained, lighted, clean of lubricants, chemicals, and waste, and easily accessible for work. The components where fluid leaks, corrosion spots, loose parts, or damaged thermal insulation have been found, shall be reported and repaired in a timely manner. | OR | Requirement for the Owner. |
| (2) The means of radiation protection, industrial safety, emergency medical services, and fire protection shall be adequately situated, well marked, and available during all operational states. Evacuation routes shall be well lighted, clearly marked, and free of all kinds of materials and objects. | OR | Requirement for the Owner. |
| (3) Operators shall be encouraged to detect and report non-conformances and shortcomings in the condition of the systems, components, and rooms. | OR | Requirement for the Owner. |
| Article 215 | | |
| (1) For identification of the SSCs, marking rules shall be established, applied, and constantly maintained. These rules shall be well known to the personnel. Those rules shall enable clear identification of each individual component and room. | COM  OR | For identification of SSCs, marking rules will be specified and applied during construction phase.  Constant maintaining and personnel training is in the responsibility of the Owner. |
| (2) Marking plates shall be suitable for the environment in which they are installed. Their form and location shall allow for clear and easy identification of the components and prevent easy removal or wrong installation. | COM/OR | Clear and easy identifiable marking plates, which are suitable for the environment, are provided. |
| (3) Marking rules shall enable the personnel to identify missing or required plates and shall ensure timely implementation of corrective actions. | COM/OR | Marking rules will be specified. |
| Article 216 | | |
| (1) The operating condition of all active components of the systems important to safety shall be documented, periodically inspected during operation, and monitored before returning to service of a power unit, scheduled annual outages, and planned changes to the reactor installation state. | OR | Requirement for the Owner. |
| (2) Specific measures shall be developed and maintained to prevent unauthorised access to or interference with the SSCs important to safety. Those measures shall include controlled access to specific rooms and zones as well as an effective control panel locking system. The measures shall not hinder the operators from effectively checking the safety system operational readiness as well as from executing quick and timely switchovers during normal operation and accident conditions. | COM | Specific measures are developed to prevent unauthorized access or interference with the SSCs important to safety, including controlled access to vital rooms and control panel locking system. The provisions for security are discussed in the AP1000 Security Design Report. |

### Section III: Maintenance, Tests, Surveillance, and Inspections. Ageing Management

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 217 | | |
| (1) During commissioning and operation, maintenance, test, surveillance, and inspection programmes shall be prepared and implemented to ensure compliance of the operability, reliability, and functionality of SSCs important to safety with the design criteria throughout the entire period of plant operation. Those programmes shall consider the operating limits and conditions and shall be revised in order to reflect operating experience. | OR/COM-B | Necessary maintenance, test, surveillance, and inspection programmes are prepared during construction phase.  Westinghouse AP1000 Equipment Reliability (ER) and Maintenance are to be used to develop this Maintenance Programs. Westinghouse Program optimizes plant safety performance and reliability. The program establishes a systematic approach to efficiently incorporate broad range of organizations, programs and processing to prevent equipment failures, and ensure high levels of safe and reliable plant operations over the lifetime of the plant.  The essential elements of the ER and Maintenance Program for the AP1000 design is to ensure ER is considered during the procurement, storage, construction, testing, and operation of new installations, and that design assumptions incorporated into the Probabilistic Safety Assessment (PSA), remain valid throughout the life of the plant. The program establishes an integrated approach to continuous improvement that prevents unanticipated failures of plant SSCs and restores degraded equipment to full capability in support of safe and reliable plant operation.  Surveillance procedures describe the procedure steps for ensuring the components functionality and availability, confirming the compliance with the established margins of the Limit Conditions of Operation and detecting any deviation before it produces an impact on the safe operation of the plant.  The surveillance procedures to be developed and provided shall be based on the surveillance requirements from the AP1000 Technical Specifications.  Westinghouse can provide inspection procedures. |
| (2) The programmes for predictive, preventive, and corrective maintenance shall cover activities for control of degradation processes, prevention of failures, and restoration of the operability and reliability of SSCs important to safety. | OR/COM-B | Maintenance programmes will include control of degradation processes, prevention of failures and restoration of the operability and reliability of SSCs important to safety.  Westinghouse has the capability to provide an Industry leading comprehensive predictive maintenance solution to efficiently maximize equipment reliability this include automated asset monitoring and maintenance group products. |
| (3) Maintenance programmes shall consider the results of the ageing management programme and cover replacement of obsolete SSCs or SSCs whose design life has expired, requalification of SSCs important to safety, and use of new maintenance technologies. | OR/COM-B | Maintenance programmes will consider again management programme. |
| (4) The programmes for periodic inspections, surveillance, and testing shall confirm either that the SSCs important to safety meet the requirements for extended safe operation, or that restoration measures are required. | OR/COM | The programmes for periodic inspections, surveillance, and testing will confirm if SSCs important to safety meet the requirements for safe operation. |
| Article 218 | | |
| (1) The scope and frequency of the maintenance, tests, surveillance, and inspections of SSCs shall be determined using a systematic approach based on:  1. Their importance to safety;  2. Their inherent reliability;  3. Their susceptibility to degradation (based on operating experience, scientific studies, and manufacturers’ recommendations);  4. Operating as well as any applicable experience and the results from the SSCs condition monitoring. | OR/COM | The scope and frequency of the maintenance, tests, surveillance, and inspections using systematic approaches based on items 1-4 in this requirement. |
| (2) Throughout the entire operating life of the NPP, the SSCs intended for prevention of practically eliminated accident sequences shall be provided with the same reliability as the one used in the design justifications. | OR | Requirement for the Owner. |
| (3) In-service inspection shall be performed at intervals determined on the basis of detection of each degradation of the most loaded component before it results in a failure. | OR/COM-B | In-service inspection programme will be specified during construction phase. |
| Article 219 | | |
| The data from maintenance, tests, surveillance, and inspections of SSCs shall be documented, stored, and analysed. Those data shall be used to detect emerging and recurrent failures as well as to revise the preventive maintenance programme. | OR | Requirement for the Owner. |
| Article 220 | | |
| (1) The maintenance programmes shall be revised periodically (at periods of less than 10 years) to reflect the operating experience. All the changes proposed shall be assessed against their effect on the SSCs’ operability, and their compliance with the relevant requirements. The maintenance total potential impact on plant safety shall also be assessed. | OR | Requirement for the Owner. |
| (2) When using the PSA methods to manage maintenance, a comprehensive and structured approach shall be adopted to identify the failure scenarios. | OR/COM | D-RAP program is presented in DCD section 17.4 to provide reasonable assurance that AP1000 is designed, procured, constructed, maintained and operated in a manner consistent with the assumptions and risk insights in the AP1000 PRA for these risk-significant SSCs.  All SSCs identified as risk significant via the design phase D-RAP are then included within the initial Maintenance Rule (MR) operational phase scope as high-safety-significant SSCs, which require increased monitoring.  The MR Administrative Program provides guidelines for implementing and complying with 10 CFR 50.65, “Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants.” The MR Program provides assurance that SSCs within the scope of the program remain reliable and capable of fulfilling their intended functions and provides processes for assessing and managing potential increases in risk that might result from proposed maintenance activities. The SSCs within the scope of the MR are summarized below:  • Safety-related SSCs  • Non-safety related SSCs that mitigate accidents or transients  • Non-safety related SSCs that are used in EOPs  • SSCs explicitly referenced in back-up or lower-tier methods in the EOPs and provides reasonable assurance of mitigation success, or whose use is implied in an EOP and essential to the completion of an EOP step  • Non-safety-related SSCs whose failure prevents safety-related SSCs from fulfilling their safety-related functions  • Non-safety-related SSCs whose failure causes scrams or actuates safety systems  After the systems and functions have been scoped, the functions are evaluated as either HSS or Low-Safety-Significant (LSS) incorporating the results of D-RAP. The safety significance classifications and bases of HSS or LSS are determined using processes consistent with Section 9.3.1 of NUMARC 93-01, “Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants.” The AP1000 D-RAP Program provides additional details for the risk determination process. |
| Article 221 | | |
| For the conduct of maintenance, tests, surveillance, and inspections jobs, working instructions shall be prepared, validated, and approved. Those instructions shall also stipulate the actions to be performed in case the obtained results deviate from the acceptance criteria. | OR/COM | Necessary maintenance, test, surveillance and inspection working instructions will be prepared, validated and approved during construction phase. |
| Article 222 | | |
| (1) During commissioning and operation, a comprehensive planning and work management system shall be applied to ensure the maintenance, tests, surveillance, and inspection activities are duly authorised, safely performed, and documented in compliance with the work procedures. | COM  OR | Planning and work management systems will be prepared during construction phase for commissioning.  The Owner is responsible for planning and work management system during operation. |
| (2) The works on SSCs important to shall be planned in a manner ensuring plant safety throughout the entire period of plant operation and complying with the operating limits and conditions. When planning works in the protected area, the principle of optimisation of the personnel radiation protection shall be applied. Operating personnel shall take an active role in the process of work planning and prioritisation. | COM  OR | Plant safety and optimization of the personnel radiation protection is ensured in all works under Supplier’s responsibility by relevant procedures, which will be specified during construction phase.  Owner is responsible for the requirement during operation. |
| (3) Authorisation of the works performance shall be granted upon a proper and adequate assessment of the personnel health hazards and plant safety resulting from the specific activity and taking into account the following specific aspects:  1. Compliance with the operating limits and conditions;  2. Isolation of the workplace, control devices, mechanical and electrical parts of the SSCs, and tagging;  3. Radiation protection, fire safety, and industrial safety measures;  4. Draining, filling, and venting of the technological systems;  5. Draining and venting means at the workplaces;  6. Monitoring of the implemented modifications. | COM  OR | Aspects presented in items 1-6 will be considered in the activities under responsibility of the Supplier.  The Owner is responsible for the requirement during operation. |
| Article 223 | | |
| Taking safety related SSCs out of service for maintenance, tests, surveillance, and inspections shall only be performed upon an authorisation by the operators in charge of the relevant SSCs. Returning SSCs to service shall be authorised by the operators upon a written confirmation that the new configuration complies with the operating limits and conditions as well as upon completion of performance tests, if required. | OR | Requirement for the Owner. |
| Article 224 | | |
| (1) Corrective maintenance of SSCs shall be planned, authorised, and executed as soon as possible and in compliance with the operating limits and conditions. Activity prioritisation depends on the defective SSCs relative importance to safety. | OR | Requirement for the Owner. |
| (2) After each operating event that has affected safety functions or the functional integrity of a component or system, a verification of the safety functions and the relevant remedial actions shall be performed, including inspections, tests, maintenance and repair, if necessary. | OR | Requirement for the Owner. |
| Article 225 | | |
| (1) The reactor coolant pressure boundary system shall be leak-tested prior to unit restart following a refuelling outage. | OR | Requirement for the Owner. |
| (2) A reactor coolant pressure boundary pressure test shall be performed at the end of each inspection period, as well as in the cases identified in the nuclear power plant design. | OR | Requirement for the Owner. |
| Article 226 |  |  |
| Surveillance measures to verify containment integrity shall cover:  1. Containment leak rate tests;  2. Individual tests of leak-tight penetrations and sealing devices, such as airlocks, doors, and isolation valves which are part of the containment, to determine their leak-tightness and, if necessary, their operability;  3. Integrity inspections of containment metal liner and prestressing tendons. | COM-B | Surveillance measures will include containment leak rate tests, individual tests of leak-tight penetrations and integrity inspections. |
| Article 227 | | |
| (1) The instruments and equipment intended for tests and studies shall be qualified and metrologically checked before use. Record keeping and validity of metrological assurance shall comply with the management system. | OR/COM-B | Necessary qualifications and metrological check with record keeping will be provided for instruments and equipment intended for tests and studies. |
| (2) The methods and procedures, instruments and personnel to be used for the reactor coolant system in-service inspection shall be qualified. | OR/COM-B | Necessary qualifications will be perfomed. |
| (3) In case of detecting unacceptable defects in the metal or new indications of defects in certain sections, additional tests shall be conducted in the problematic section and other analogous sections. The scope for further tests shall depend on the defects’ nature and extent to which they influence the assessments of nuclear safety and potential consequences. | OR/COM | If there are unacceptable defects or indications of defects, additional tests will be conducted to the scope necessary. |
| Article 228 | | |
| (1) The operating organisation shall prepare, implement, assess, and improve an ageing management programme to identify all the mechanisms for ageing of SSCs important to safety, their possible consequences as well as the required actions to maintain the SSCs’ operability and reliability. | OR | Requirement for the Owner. |
| (2) All SSCs important to safety shall be assessed in terms of performance of intended safety functions throughout their design life taking into account the ageing and wear mechanisms as well as possible degradation resulting from the time of operation and load cycles. | OR | Requirement for the Owner. |
| (3) Environmental conditions, process parameters, maintenance and test schedules, and strategy for replacement of SSCs important to safety shall be considered factors in ageing management. | OR | Requirement for the Owner. |
| (4) Monitoring, testing, sampling, and inspections shall be conducted to evaluate ageing effects and early detection of unanticipated behaviour or degradation. | OR | Requirement for the Owner. |
| Article 229 | | |
| The ageing management programme shall be assessed and updated at least during the periodic safety review to include new information and emerging problems, use advanced methods and tools, and assess the maintenance practice used. | OR | Requirement for the Owner. |
| Article 230 | | |
| (1) Ageing management of the reactor pressure vessel and its welding seams shall consider all relevant factors, including radiation embrittlement, thermal ageing and fatigue, and shall compare their evolution throughout the plant design life with the design limits. | OR | Requirement for the Owner. |
| (2) Surveillance of major structures and components shall detect in a timely manner the initial phases of ageing processes in order to reduce preventive and remedial actions. | OR | Requirement for the Owner. |

### Section IV: Radiation Protection During Operations

| **Requirement** | **Category** | **Compliance Assessment Description** |
| --- | --- | --- |
| Article 231 | | |
| Before commissioning of a nuclear power plant, a Radiation Protection Programme and Environmental Radiological Monitoring Programme shall be prepared and approved by the national competent authorities. Throughout the operation of an NPP, the programmes shall be periodically reviewed and updated based on the operating experience. | OR | Requirement for the Owner. |
| Article 232 | | |
| (1) The Radiation Protection Programme for the personnel shall be aimed at limiting the personnel dose exposure below the authorised limits and as low as reasonably achievable during all operational states of the plant. | OR | Requirement for the Owner. See additional considerations in the assessment BGP-GW-GL-202[7]. |
| (2) Compliance with the Radiation Protection Programme as well as the accomplishment of its objectives shall be verified based on surveillance, inspections, and audits. | OR | Requirement for the Owner. |
| Article 233 |  |  |
| The Radiation Protection Programme for the personnel shall be based on a preliminary analysis of the radiological risk which shall consider the zones and proportions of the radiological hazards and shall cover:  1. Classification of radiation zones and access control;  2. Internal regulations and activity surveillance at the radiation zones;  3. Personnel and workplace radiation monitoring;  4. Planning of activities and work authorisations at the radiation zones;  5. Collective and personal protective equipment;  6. Facilities, shielding materials, and radiation protection equipment;  7. Personnel medical surveillance;  8. Application of the protection optimisation principle;  9. Reduction of ionising radiation sources;  10. Radiation protection training;  11. Emergency response actions. | OR | Requirement for the Owner. |
| Article 234 | | |
| (1) The limits on liquid and gaseous radioactive discharges stipulated in the Technical Specifications shall be based on an assessment of their radiological effect on representative members of the public using modelling of the anticipated exposure doses in relation to the distance from the NPP, food and drinking water consumption, sources of food and drinking water, and all local customs and practices which may cause exposure doses higher than the average. | OR | Requirement for the Owner. See additional considerations in the assessment BGP-GW-GL-202[7]. |
| (2) The limits on liquid and gaseous radioactive discharges shall be monitored at the sources of those discharges and verified through environmental measurements. Three types of measurements can be used for source monitoring:  1. Online discharge monitoring;  2. Continuous sampling and laboratory measurements of sample activity;  3. Periodical sampling and laboratory measurements of sample activity. | OR/COM-B | Radiation monitoring system is presented in DCD section 11.5, including liquid and gaseous effluent monitors.  The gaseous radwaste and liquid radwaste processing systems also include continuous radiation monitoring of their discharge paths.  Sampling systems are described in DCD section 9.3.  Design features to control airborne radioactivity is presented in DCD section 12.3.  The design has considered this requirement. AP1000 plant is designed in a way that all liquid and gaseous release points are monitored using continuous radiation monitoring system RMS. AP1000 Effluent monitoring for Bulgaria shall be in agreement with local requirements, thus most likely it should conform with Recommendation 2004/2/Euratom which provides guidance to EU countries on the reporting of discharges of radioactive nuclides. |
| (3) The type of measurement to be chosen for source monitoring shall depend on the source term, sensitivity of the measuring system, anticipated discharge variations in time, and potential for unplanned discharges requiring timely detection and notification. | OR/COM | The type of measurement is chosen based on its suitability, see e.g., DCD section 11.5.2.3.3 for plant vent radiation monitor. |
| Article 235 | | |
| (1) The Environmental Radiological Monitoring Programme under Article 231 shall be implemented at least two years prior to commissioning of an NPP. The programme shall cover measurement of the radiation background in the vicinity of the plant and its seasonal fluctuations, sampling and analysing the radionuclide content of samples of vegetables, air, milk, water, sediments, fish, soil, and plants from several spots identified off the plant site. | OR | Responsibility of the Owner. |
| (2) The Environmental Radiological Monitoring Programme shall provide information for the purpose of:  1. Verifying the adequacy of the radioactive discharges monitoring;  2. Comparing environmental radiological monitoring data with radioactive discharge source monitoring data;  3. Checking the validity of the environmental models used to determine the authorised limits of radioactive discharges;  4. Strengthening public trust;  5. Evaluating the trends in the concentrations of radionuclides in the environment. | OR | Responsibility of the Owner. |
| Article 236 | | |
| (1) Throughout the operation of an NPP, generation of radioactive waste shall be kept as low as possible in terms of both activity and scope based on the appropriate operating practice. | OR | Responsibility of the Owner.  The AP1000 plant design conforms with the principles of waste management as far as practicable and fulfils these requirements. The minimization of radwaste is typically strongly dependent on the operational programs implemented within any given plant (specifically in dry wastes). From a reactor design standpoint, appropriate measures have been taken to minimize the production of radwaste. These include proven radwaste treatment techniques and minimization of plant source term through appropriate materials selection. Material specifications related to source term reduction are described under “Materials” in subsection 12.3.1.1.1 and in Table 12.3-1 of the DCD.  As discussed throughout DCD Chapter 11, the AP1000 standard plant design provides appropriate design provisions for the management of liquid and gaseous radwaste for the entire lifecycle (generation, segregation, collection, treatment, and controlled discharge).  Appropriate design provisions are provided for the solid radwaste lifecycle up to the collection phase. The AP1000 standard plant design does not include provisions for packaging or volume reduction of solid radwaste. The final selection of the packaging and treatment solutions will be performed as part of site-specific project development. |
| (2) The structures, systems, and components used to treat and store radioactive waste throughout the operation of the plant shall be maintained in an operable condition and monitored through the maintenance, surveillance, test, and inspection programmes. | OR | Responsibility of the Owner. |
| (3) Accumulation of large quantities of untreated radioactive waste as well as their prolonged temporary storage outside the design facilities shall be avoided. | OR | Responsibility of the Owner. |
| (4) Radioactive wastes shall be characterised at all stages of their management throughout the operation of the plant. The process of characterisation shall cover the measurement of physical and chemical parameters, source term, and specific activity. | OR | Responsibility of the Owner. |
| (5) Variations in the radioactive waste characteristics during their storage shall be monitored through inspections and periodic analyses. | OR | Responsibility of the Owner. |
| (6) RAW treatment and storage shall provide for their removal from the facilities at the end of their storage period. | OR | Design provides possibility to remove RAW from the facilities at the end of their storage period, see DCD section 11. |
| (7) Throughout the operation of an NPP, the relevant margins shall be ensured in the RAW storage facilities in case of unanticipated circumstances. The facilities’ fill-up level shall be monitored and, if necessary, actions shall be taken to recover the margins. | OR/COM | Instrumentation is provided to monitor fill-up level of the waste tanks, see DCD section 11.2. |
| (8) The On-Site Emergency Plan of an NPP shall provide for the storage of large quantities of liquid radioactive waste in the event of a core melt accident or damage of the spent nuclear fuel stored at the plant. | OR | Requirement for the Owner. |
| Article 237 | | |
| (1) The administrative unit assigned to control the radiation protection during the operation of an NPP shall have sufficient independence and required resources to be able to efficiently apply the optimisation principle, propose and monitor the internal radiation exposure limits, and take actions to comply with the radiation protection regulations at all levels of the operating organisation. | OR | Responsibility of the Owner. |
| (2) The plant management shall identify mechanisms for including the personnel into the development of methods for maintaining the personnel and public radiation exposure doses as low as reasonably achievable and shall provide feedback on the efficiency of the radiation protection measures. | OR | Responsibility of the Owner. |
| (3) Plant and contractors’ personnel shall be aware of the radiological hazards of the activities being performed and shall bear personal responsibility for putting into practice the personal protective measures. | OR | Responsibility of the Owner. |
| (4) Plant personnel shall be recruited in advance and subjected to periodical medical examinations in order to verify their physical and psychophysiological fitness for the relevant job positions. | OR | Responsibility of the Owner. |

# SUMMARY AND CONCLUSIONS

## OVERALL HIGH LEVEL RISK ASSESSMENT

Given the analyses performed in Part 4. The Bulgarian Regulation on Ensuring the Safety of Nuclear Power Plants is Classified as Medium Risk.

## IDENTIFIED POTENTIAL RISK TO BE ADDRESSED IN BULGARIA PROJECT

Following topics presented in the table below, are considered as **“CWO” – Compliant with Objective:**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Related Articles (subarticles)** | **Justification** |
| Defense in Depth. SSCs independency | 41 (4), 57 (1), 112 (3) | There are SSCs which are used both during transients and during accidents with fuel melting, such as Passive Containment Cooling System. However, operation of these systems during transients does not affect the operation during accidents with fuel melting.  Due to the passive features with high reliability in AP1000 design, it is considered that objective of this requirement is met. This is confirmed by deterministic and probabilistic safety analyses (DCD sections 15 and 19).  No design changes to AP1000 standard design or additional analyses are expected |
| Multiple failures | 49 (2) | Common cause failures are considered in AP1000 design by introducing diversified safety functions and SSCs to strengthen the defense-in-depth concept, e.g., diverse means for core cooling, diversity in automatic depressurization and diversity in actuation system.  Common cause analysis is included in the AP1000 plant PRA as stated in the AP1000 plant DCD Section 19.29. The PRA was used to define where and to what degree diversity needed to be incorporated into the AP1000 plant SSCs.  No design changes to AP1000 standard design or additional analyses are expected |
| Safety Classification | 54 (2-4) | Safety classification principles for AP1000 design is presented in DCD section 3.2. The classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements. The classification of SSCs is slightly different than required in this article, e.g., safety class C includes components, which provides safety support functions to Class A, B and C SSCs.  The AP1000 classification system provides a means of identifying the extent to which structures, systems, and components are related to safety-related and seismic requirements. The classification system provides an easily recognizable means of identifying the extent to which structures, systems, and components are related to ANS nuclear safety classification, NRC quality groups, ASME Code, Section III classification, seismic category, and other applicable industry standards, as shown in DCD table 3.2-3.  No design changes to AP1000 standard design or additional analyses are expected. |
| Site-specific hazards and Extreme Events. | 84 (2) | External hazards are considered in AP1000 design, e.g., in DCD section 3.7 (seismic), flooding (section 3.4), wind and tornado loadings (section 3.3) and malevolent aircraft impact (appendix 19F).  No design changes to AP1000 standard design are expected, however site-specific hazards may require further consideration/analysis in the safety assessment. |
| Remote shutdown station | 114 (3), 211 (1) | The remote shutdown workstation is provided for control of the plant in the case of an evacuation of the main control room (mainly due to fire). The remote shutdown station is not needed for other internal and external events.  Additionally, a secondary diverse actuation is in a diverse spatially separated location (not in the same zone of the plant) to actuate key safety functions such as ADS Stage 4 actuation, IRWST injection and containment recirculation actuation. The secondary DAS panel is powered by an independent local battery. The secondary DAS panel is located sufficiently far from the Main Control Room (MCR) and Remote Shutdown Workstation), its location has been selected as to provide additional protection so that it is very unlikely that it could be affected by internal events such as fire, internal flooding, or external events such as flooding (thus providing additional protection from these events).  This is considered complying with the objective, hence, no design changes to AP1000 standard design is expected. This topic is proposed to be follow-up to ensure this approach and discard potential additional analyses or design change. At this stage this is considered a Medium Risk. |
| Containment isolation for 4 instrument lines. | 130 (1) | Containment Isolation related to four instrumentation lines is demonstrated according to Regulatory Guide 1.11. and alternate criteria.  No design changes to AP1000 standard design or additional analyses are expected |
| Support functions own protections | 137 (4) | Due to the passive features of the AP1000 design, the number of supporting safety systems needed for accident management is limited, since main safety functions are performed by passive systems. Thus, active components are not classified as safety related to perform safety functions (they are included in the Defense in Depth type of Systems, thus not safety-related), for the previous reason the need to preclude their own protections is not as relevant and is to be analyzed only for Probabilistic Analyses.  No design changes to AP1000 standard design or additional analyses are expected. |
| Commissioning tests | 173 (1-2) | Commissioning tests will be provided as presented in DCD section 14. Test program will cover all necessary tests but with different test structure.  No design changes to AP1000 standard design or additional analyses are expected |

Following topics are considered as **COM-B – “Compliant with planned update for Bulgaria Units”:**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Related Articles (subarticles)** | **Justification** |
| Radiation impact | 2 (1), 4 (3), 43 | Additional Analyses Needed.  DCD chapter 12 provides principles to ensure that radiation impact is kept as low as reasonably achievable. This has been assessed in reference [7] as COM-B since it is recognized that new analyses need to be performed. Due to comprehensive consideration of design features to limit radiation exposures (see e.g., DCD section 12), it is expected that there is no need for design changes. However, this needs to be confirmed with the analyses. |
| Site compatibility | 3 (1), 4 (3), 28 | Additional Analyses Needed.  The compatibility of the site and site conditions are studied in report KZG-GW-GL-100 [9] and related to seismic and geotechnics in report KZG-GE01-X7R-001 [10]. Full compatibility of the proposed units with the conditions on site will need to be demonstrated taking into consideration the recommendations in these reports. |
| Multiple NPP’s on site | 30 (2), 174 | Additional Analyses Needed.  Selected site includes existing nuclear facilities. This may need further considerations in the design and safety analyses. |
| Aircraft crash | 33 (5), 85, 86 | Westinghouse has performed a rigorous assessment of the AP1000 plant design to demonstrate that the plant’s design features, and functional capabilities provide inherent protection against the effects of an aircraft impact, this assessment count with regulatory approvals that will need to be validated by BNRA. . |
| Probabilistic Risk Analysis (PRA) need for Additional Analyses | 44 (2), 49 (6), 79 (1-4) | Additional Analyses Needed.  External hazards are considered in the AP1000 design by structural design solutions and passive design features. Similarly, spent fuel pool design is designed so that structural integrity is always confirmed and spent fuel pool cooling is always ensured. For these reasons, it is expected that there are no design changes needed in AP1000.  Probabilistic safety analyses are documented in DCD section 19, and it confirms that AP1000 design is robust against different initiating events and hazards with high safety margin. However, these topics may require further development needs in the PRA models and analyses. In addition, site-specific data may require adjustments in the PRA models. |
| Site specific hazards and conditions | 33(5), 80 (5), 81, 83 (4, 6-7), 125 (3) | Additional Analyses Needed.  Each site has its specific characteristics, and it shall be confirmed that all hazards are considered in the design. Due to robust design solutions for AP1000, it is expected that there will be no major design changes needed due to site-specific characteristics and hazards. However, this may require new analyses to confirm that there are no hazards which could affect the safety of the AP1000.  See recommendations on references [9] and [10]. |
| Inspection, maintenance, testing | 168 (1), 169 (1-3), 170 (1-2), 171, 172 (1-2), 173 (3-4), 217 (1-3), 218 (3), 221 (1-2), 226 (1), 227 (1-2) | Specific/Additional Documentation might need to be produced.  AP1000 plant meets the design related to taking into consideration inspection and maintenance programs. Nonetheless the licensee shall prepare and implement documented programs of maintenance, testing, surveillance, and inspection of SSCs important to safety.  Westinghouse will provide input to the designer for maintenance, testing, surveillance, and inspection developed for AP1000 plant SSCs for the Owner to develop their programs.  The initial test program is described in DCD chapter 14. Detailed commissioning programme will be specified more in detail during the construction phase. |
| Operating Procedures, Emergency procedures & SAMGs | 188 (2-3), 189 (1-2), 190 (1-3), 191 (1-2), 192 (1-2), 203 (2-3), 206 (2) | Specific/Additional Documentation might need to be produced. No design Changes to Standard Design expected.  Emergency procedures and SAMGs are prepared during the construction phase. Standard AP1000 Procedures will be used as input. |
| Chemistry program | 213 (1-2) | Specific/Additional Documentation might need to be produced. No design Changes to Standard Design expected.  The chemistry program shall be prepared during the construction phase. It will be based on AP1000 standard Chemistry Manual, procedures, and specifications. |
| Effluent monitoring | 234 (2) | AP1000 plant is designed in a way that all liquid and gaseous release points are monitored using continuous radiation monitoring system RMS. AP1000 Effluent monitoring for Bulgaria shall be in agreement with local requirements, thus most likely it should conform with Recommendation 2004/2/Euratom which provides guidance to EU countries on the reporting of discharges of radioactive nuclides. |

Other Topics of interest on the Assessment:

* Article 139(2): Fire response class A1 or A2 is required this has been Classified as NAS Not Assessable, this might need to be studied to understand it potential impact, at this moment it is understood as low Risk since AP1000 Fire protection Approach is expected to be maintained..

The AP1000 design is protected against internal and external fires, see e.g., DCD Appendix 9A, where fire protection analysis is performed. For that reason, it is expected that there is no need for changes regarding fire protection. However, it needs to be understood if currently applied fire response class ratings comply with classes A1 and A2.

* Article 147(4):.specifies that “The design shall specify the way for management of large quantities of liquid RAW generated in accident conditions”. This has been classified as owner requirement, since it does not affect AP1000 Standard Design. However the exten of this requirement could potentially added some additional scope that is currently not considered, this needs to be fully understood..

The rest of the regulation can be classified as Low Risk.

# REFERENCES

1. “Regulation on Ensuring the Safety of Nuclear Power Plants” L.KNP\_WEC\_230003, 8th of June 2023
2. APP-GW-GL-700, Revision 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, Revision 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, Revision 8, “AP1000 Probabilistic Risk Assessment”, Westinghouse Electric Company
5. APP-GW-GL-900, Revision 0, “AP1000 Plant Methodology for Demonstration of Practical Elimination”, Westinghouse Electric Company
6. BGP-GW-GL-201, Revision A, “Assessment of the AP1000 Plant for the Bulgarian Act on the Safe Use of Nuclear Energy.”
7. BGP-GW-GL-202, Revision A, “Assessment of the AP1000 Plant for the Bulgarian Regulation on Radiation Protection.”
8. BGP-GW-GL-205, Revision A, “Assessment of the AP1000 Plant for the Bulgarian Regulation Related to Safe Management of Radioactive Waste
9. KZG-GW-GL-100, Revision 0, “AP1000 Technical Risk Assessment of the PSAR, Site Assessment and Site Approval Order for Kozloduy Site”
10. KZG-GE01-X7R-001, Revision A, “Preliminary Report of Available Geotechnical Data, Assessment of the Compatibility of the Site with Seismic Envelope Parameters for AP1000 and Recommendations for Future Characterization Activities”
11. NPP\_NPP\_000065, Revision 0, AP1000 Nuclear Power Plant Coping with Station Blackout
12. NPP\_NPP\_000067, Revision 0, AP1000 Nuclear Power Plant Spent Fuel Pool Cooling
13. NPP\_NPP\_000072, Revision 0, Westinghouse AP1000 Nuclear Power Plant Response to External Hazards
14. ACT ON THE SAFE USE OF NUCLEAR ENERGY Promulgated, State Gazette No. 63/28.06.2002, amended and supplemented, SG No. 120/29.12.2002, SG No. 70/10.08.2004, effective 1.01.2005, amended, SG No. 76/20.09.2005, effective 1.01.2007, SG No. 88/4.11.2005, SG No. 105/29.12.2005, effective 1.01.2006, SG No. 30/11.04.2006, effective 12.07.2006, SG No. 11/2.02.2007, amended and supplemented, SG No. 109/20.12.2007, effective 1.01.2008, amended, SG No. 36/4.04.2008, SG No. 67/29.07.2008, amended and supplemented, SG No. 42/5.06.2009, amended, SG No. 74/15.09.2009, effective 15.09.2009, amended and supplemented, SG No. 80/12.10.2010, amended, SG No. 87/5.11.2010, SG No. 88/9.11.2010, effective 1.01.2011, SG No. 97/10.12.2010, effective 10.12.2010, SG No. 26/29.03.2011, effective 30.06.2012, SG No. 38/18.05.2012, effective 1.07.2012, SG No. 82/26.10.2012, effective 26.11.2012, amended and supplemented, SG No. 15/15.02.2013, effective 1.01.2014, amended, SG No. 66/26.07.2013, effective 26.07.2013, SG No. 68/2.08.2013, effective 2.08.2013, SG No. 98/28.11.2014, effective 28.11.2014, SG No. 14/20.02.2015, SG No. 58/18.07.2017, effective 18.07.2017, SG No. 99/12.12.2017, effective 1.01.2018, amended and supplemented, SG No. 102/22.12.2017, effective 1.01.2018, supplemented, SG No. 103/28.12.2017, effective 1.01.2018, amended, SG No. 7/19.01.2018, SG No. 77/ 18.09.2018, effective 1.01.2019 amended and supplemented SG No. 17/25.02.2020.
15. Regulation on the Procedure for Issuing Licenses and Permits for the Safe Use of Nuclear Energy Promulgated, SG No. 41/18.05.2004 Amended and supplemented, SG No. 78/30.09.2005; 93/24.11.2009; 76/05.10.2012; 4/15.01.2016; 4/9.01.2018; 37/ 4.05.2018; 53/5.07.2019.
16. Regulation on Radiation Protection. Promulgated, State Gazette SG No. 16/2018; amended and supplemented, State Gazette SG No. 110/2020.
17. Regulation on Ensuring the Safety of Spent Nuclear Fuel Management adopted by CM Decree No. 196 of 02 August 2004, promulgated, SG No. 71 of 13 August 2004, amended SG No. 76 of 30 August 2013, amended SG No. 4 of 09 January 2018, in force as of 09 January 2018, No. 37 of 04 May 2018.
18. Regulation on Safe Management of Radioactive Waste adopted by CM Decree No. 185 of 23 August 2013, promulgated, SG No. 76 of 30 August 2013, amended SG No. 4 of 09 January 2018, in force as of 09 January 2018, No. 37 of 04 May 2018.
19. Bulgarian Nuclear Regulatory Agency Order No. АА-04-30. 21.02.2020. By which BNRA Approves: "the site selected by KOZLODUY NPP – NEW BUILDS PLC (UIC 202058513) for the siting of a nuclear facility - nuclear power plant (Site No. 2) with a location, boundaries and characteristics according to the submitted documents."
20. Council Directive 2014/87/EURATOM of 8 July 2014 amending Directive 2009/71/Euratom Establishing a Community Framework for the Nuclear Safety of Nuclear Installations.
21. TD-WES-13-002 PART II Revision 2. Feasibility Study for the Construction of a New Nuclear Unit at Kozloduy NPP Site. PART II. Revision 2. "Assessment of the Characteristics and Condition of the Proposed Sites. Comparative Analysis and Proposal for Site Selection." July 2013.
22. NPP\_NPP\_000067, Revision 0. “AP1000® Nuclear Power Plant Spent Fuel Pool Cooling.” May 2011.
23. APP-GW-G0R-003, Revision A, “Compliance Assessment of the IAEA Specific Safety Guide SSG-61 “Format and Content of the Safety Analysis Report for Nuclear Power Plants””.
24. APP-GW-GL-059, Revision A. Compliance Assessment of the IAEA Specific Safety Guide SSG-61 “Format and Content of the Safety Analysis Report for Nuclear Power Plants”.
25. EPS-GW-GL-701, Revision C. AP1000 Plant Evaluation of Western European Nuclear Regulators’ Association Safety Objectives for New Power Reactors.
26. APP-GW-G0R-006, Revision A. Assessment of the AP1000 Plant to IAEA Specific Safety Guide No. SSG-34 "Design of Electrical Power Systems.
27. L.WEC\_KNP\_230019, “Meeting Minutes from Completion of FEED Deliverables D.02.04 Meeting Minutes of Video conference workshop 1 on applicable regulations, regulatory guides, codes and standards for the Kozloduy Unit 7 new build project.” 8 September 2023.
28. L.WEC\_KNP\_230025, “Action Items from Deliverable 02.04 Workshop”. 18 October 2023
29. BGP-GW-GEH-001, Revision A, “Preliminary Radioactive Waste Information for Bulgaria”.
30. BGP-GW-GL-204, Revision C, “Assessment of the Bulgarian AP1000 Plant Project with Regard to the Bulgarian Regulation on Ensuring the Safety of Spent Nuclear Fuel Management”.
31. APP-GW-G0R-010, Revision A, “Assessment of the AP1000 Plant to IAEA Specific Safety Guide No.SSG-54 "Accident Management Programmes for Nuclear Power Plants”.