HITACHI

GE Hitachi Nuclear Energy

NEDO-34165
Revision A
January 2025

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

BWRX-300 UK Generic Design Assessment (GDA) Chapter 3 - Safety Objectives and Design Rules for Structures, Systems and Components

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

NEDO-34165 Revision A

INFORMATION NOTICE

This document does not contain proprietary information and carries the notations “US Protective Marking: Non-Proprietary Information” and “UK Protective Marking: Not Protectively Marked.”

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT
Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purpose of obtaining the applicable Nuclear Regulatory Authority review and determination of acceptability for use for the BWRX-300 design and licensing basis information contained herein. The only undertakings of GEH with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, no representation or warranty is provided, nor any assumption of liability is to be inferred as to the completeness, accuracy, or usefulness of the information contained in this document. Furnishing this document does not convey any license, express or implied, to use any patented invention or any proprietary information of GEH, its customers or other third parties disclosed herein or any right to publish the document without prior written permission of GEH, its customers or other third parties.

UK SENSITIVE NUCLEAR INFORMATION AND US EXPORT CONTROL INFORMATION

This document does not contain any UK Sensitive Nuclear Information (SNI) subject to protection from public disclosure as described in the Nuclear Industries Security Regulations (NISR) 2003, does not contain UK Export Controlled Information (ECI), and does not contain US Export Controlled Information (ECI) subject to the export control laws and regulations of the United States, including 10 CFR Part 810.

EXECUTIVE SUMMARY

The purpose of this Preliminary Safety Report (PSR) chapter is to present the general Safety Objectives and Design Rules for Structures, Systems and Components (SSCs) used in the design and assessment of the Boiling Water Reactor (BWR) BWRX-300 reactor design.

This chapter, along with its Attachment, outlines the general design concepts, requirements, codes and standards applicable for different kinds of SSCs and the approach adopted to meet the safety objectives. The compliance of the actual design with all these elements is demonstrated in further detail in other chapters of the PSR, in particular in those devoted to a description of different SSCs.

This chapter presents a level of detail commensurate with a 2-step Generic Design Assessment (GDA) and is structured in line with the high-level contents of International Energy Atomic Agency SSG-61.

The safety objectives and design rules presented in this chapter cover safety functions and functional requirements, radiological acceptance criteria, the Defence-in-Depth (D-in-D) and Defence Lines (DLs) concept and its application, application of general design requirements, and SSCs categorisation and classification. These have been outlined based on international Relevant Good Practice (RGP).

This chapter and its Attachment, presents relevant information on the design approaches to civil engineering and design of seismic category buildings and structures, mechanical components, instrumentation and control systems, and electrical systems and components.

This chapter sets out the approach to equipment qualification and an overview of the codes and standards applicable to in-service monitoring, testing, maintenance, and inspections.

Claims and arguments relevant to GDA Step 2 objectives and scope are summarised in Appendix A, along with an As Low As Reasonably Practicable position. Appendix B provides a Forward Action Plan, which includes future work commitments and recommendations for future work where ‘gaps’ to GDA expectations have been identified. UK-specific context information is provided in Appendix C.

ACRONYMS AND ABBREVIATIONS

Acronym	Explanation
AC	Alternating Current
AISC	American Institute of Steel Construction
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
AOO	Anticipated Operational Occurrence
API	American Petroleum Institute
ASCE(/SEI)	American Society of Civil Engineers (/Structural Engineering Institute)
ASME	American Society of Mechanical Engineers
AWWA	American Water Works Association
BDBA	Beyond Design Basis Accident
BPVC	(ASME) Boiler Pressure Vessel Code
BSL	Basic Safety Limit
BSO	Basic Safety Objective
BWR	Boiling Water Reactor
CAE	Claims, Arguments, Evidence
CB	Control Building
CCF	Common Cause Failure
CIV	Containment Isolation Valve
CRD	Control Rod Drive
DBA	Design Basis Accident
DBE	Design Basis Earthquake
DC	Direct Current
DCIS	Distributed Control and Information System
DEC	Design Extension Condition
D-in-D	Defence-in-Depth
DL	Defence Line
DL1	Defence Line 1
DL2	Defence Line 2
DL3	Defence Line 3
DL4	Defence Line 4
DL4a	Defence Line 4a
DL4b	Defence Line 4b
DL5	Defence Line 5
EMC	Electromagnetic Compatibility
EMI/RFI	Electromagnetic/Radio Frequency Interference
EQ	Environmental Qualification

Acronym	Explanation
FMEA	Failure Modes and Effects Analyses
FSF	Fundamental Safety Function
GDA	Generic Design Assessment
GEH	GE Hitachi Nuclear Energy
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INSAG	International Nuclear Safety Advisory Group
ISI	Inservice Inspection
ISRS	In-Structure Response Spectra
IST	In-Service Testing
LfE	Learning from Experience
LV	Low Voltage
LWR	Light Water Reactor
MCR	Main Control Room
MSQA	Management of Safety and Quality Assurance
MV	Medium Voltage
NDE	Non-Destructive Examination
NPP	Nuclear Power Plant
OLC	Operational Limit and Condition
OM	Operations and Maintenance of Nuclear Power Plants
ONR	(UK) Office for Nuclear Regulation
OPEX	Operational Experience
PAM	Post-Accident Monitoring
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Assessment
PSR	Preliminary Safety Report
RB	Reactor Building
RBV	Reactor Building Vibration
RCPB	Reactor Coolant Pressure Boundary
RG	Regulatory Guide
RGP	Relevant Good Practice
RPV	Reactor Pressure Vessel
RRS	Required Response Spectra
SAPs	(ONR) Safety Assessment Principles

Acronym	Explanation
SC	Safety Class
SC1	Safety Class 1
SC2	Safety Class 2
SC3	Safety Class 3
SMR	Small Modular Reactor
SSCs	Structures, Systems and Components
SSE	Safe Shutdown Earthquake
TEMA	Tubular Exchanger Manufacturers Association
UK	United Kingdom
U.S.	United States
USNRC	U.S. Nuclear Regulatory Commission

TABLE OF CONTENTS

EXECUTIVE SUMMARY iii

ACRONYMS AND ABBREVIATIONS iv

3. SAFETY OBJECTIVES AND DESIGN RULES FOR STRUCTURES, SYSTEMS AND COMPONENTS 1

3.1. General Safety Design Basis 4

3.2. Categorisation of Functions and Classification of Structures, Systems and Components 26

3.3. Protection Against External Hazards 33

3.4. Protection Against Internal Hazards 34

3.5. Design of Civil Structures 35

3.6. Mechanical Systems and Components 36

3.7. General Design Aspects for Instrumentation and Control Systems and Components 37

3.8. General Design Aspects for Electrical Systems and Components 38

3.9. Equipment Qualification 39

3.10. Inservice Monitoring, Tests, Maintenance, and Inspections 53

3.11. Compliance with National and International Standards 55

3.12. References 63

APPENDIX A CLAIMS, ARGUMENTS AND EVIDENCE 69

APPENDIX B FORWARD ACTIONS 74

APPENDIX C UK SPECIFIC CONTEXT INFORMATION 75

LIST OF TABLES

Table 3-1: Identification of Defence Levels 57
Table 3-2: Safety Category for Functions Based on Defence Line Assignment 58
Table 3-3: Codes and Standards for Pressure-Retaining Equipment 59
Table A-1: Safety Objectives and Design Rules for SSCs Claims and Arguments 71

LIST OF FIGURES

Figure 3-1: Defence-in-Depth - Plant States and Defence Lines 61
Figure 3-2: BWRX-300 Safety Strategy Implementation Process 62

NEDO-34165 Revision A

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
A	All	Initial Issuance

3. SAFETY OBJECTIVES AND DESIGN RULES FOR STRUCTURES, SYSTEMS AND COMPONENTS

Introduction

Preliminary Safety Report (PSR) Ch. 3 presents the safety design basis of the BWRX-300 in a United Kingdom (UK) context. It provides a description of As Low As Reasonably Practicable (ALARP); dose targets and limits; the Defence in Depth (D-in-D) principle and its application; deterministic design principles; equipment qualification and aging. PSR Ch. 3 also summarise Categorisation and Classification methodology.

PSR Ch. 3 and its Attachment 1 (Reference 3-1) cover general principles and do not include the detailed analyses and substantiation by which each specific area is evaluated.

PSR Ch. 3 presents a level of detail commensurate with a 2 Step Generic Design Assessment (GDA) and is structured in line with the high level contents of International Atomic Energy Agency (IAEA) SSG-61, "IAEA Safety Standards – Format and Content of the Safety Analysis Report for Nuclear Power Plants," (Reference 3-2).

Purpose

PSR Ch. 3 introduces the safety objectives and the safety strategy to meet those objectives for the design and construction of the BWRX-300 in the UK.

Additionally, PSR Ch. 3 describes the methodology for classification of Structures, Systems, and Components (SSCs), the general design aspects, and codes, standards, and RGP applied to the BWRX-300 design to meet the UK regulatory requirements.

Interfaces with Other Chapters

The interfaces between PSR Ch. 3 and other chapters in the PSR are presented as follows:

- NEDC-34166P, "BWRX-300 UK GDA Ch. 4: Reactor (Fuel and Core)," (Reference 3-3), NEDC-34167P, "BWRX-300 UK GDA Ch. 5: Reactor Coolant System and Associated Systems," (Reference 3-4), NEDC-34168P, "BWRX-300 UK GDA Ch. 6: Engineered Safety Systems," (Reference 3-5), NEDC-34169P, "BWRX-300 UK GDA Ch. 7: Instrumentation and Control," (Reference 3-6), NEDC-34170P, "BWRX-300 UK GDA Ch. 8: Electrical Power," (Reference 3-7), and NEDC-34171P, "BWRX-300 UK GDA Ch 9A: Auxiliary Systems," (Reference 3-8) – These chapters present the design of systems and components which are based on the relevant safety and design principles provided in PSR Ch. 3.
- NEDC-34172P, "BWRX-300 UK GDA Ch. 9B: Civil Structures," (Reference 3-9) – presents the design of civil engineering works and structures which is based on the relevant principles presented in PSR Ch. 3.
- NEDC-34173P, "BWRX-300 UK GDA Ch. 10: Steam and Power Conversion Systems," (Reference 3-10) – presents the design of the steam and power conversion systems which is based on the relevant safety and design principles presented in PSR Ch. 3.
- NEDC-34174P, "BWRX-300 UK GDA Ch. 11: Management of Radioactive Waste," (Reference 3-11) – presents the design of systems and components containing radioactive materials based on the safety and design principles provided in PSR Ch. 3.
- NEDC-34175P, "BWRX-300 UK GDA Ch. 12: Radiation Protection," (Reference 3-12) – presents the design of radiation protection based on the safety and design principles presented in PSR Ch. 3.
- NEDC-34176P, "BWRX-300 UK GDA Ch. 13: Conduct of Operations," (Reference 3-13) – uses the relevant engineering substantiation principles presented

in PSR Ch. 3 to develop the operational conduct and management for the UK BWRX-300.

- NEDC-34177P, "BWRX-300 UK GDA Ch. 14: Plant Construction and Commissioning," (Reference 3-14) – presents the arrangements and requirements for plant construction and commissioning, considering the relevant principles presented in PSR Ch. 3.
- PSR Ch. 15 – Safety Analysis (References 3-15 through to 3-24) – provides the overarching safety analysis including Probabilistic Safety Assessments (PSAs), Design Basis Analyses (DBAs), and Beyond Design Basis Accidents, including Design Extension Conditions and severe accidents, with the consideration of relevant principles presented in PSR Ch. 3.
- NEDC-34188P, "BWRX-300 UK GDA Ch. 16: Operational Limits and Conditions," (Reference 3-25) – uses the relevant engineering substantiation principles presented in PSR Ch. 3 to develop the operational limits and conditions for the UK BWRX-300.
- NEDC-34189P, "BWRX-300 UK GDA Ch. 17: Management for Safety and Quality Assurance," (Reference 3-26) – presents codes and standards applied to Management of Safety and Quality Assurance (MSQA) which is based on the selection principles of codes and standards in PSR Ch. 3.
- NEDC-34190P, BWRX-300 UK GDA Ch. 18: Human Factors Engineering," (Reference 3-27) – presents the substantiation of Human Factors principles which are provided in PSR Ch. 3.
- NEDC-34191P, "BWRX-300 UK GDA Ch. 19: Emergency Preparedness and Response," (Reference 3-28) – presents the emergency preparedness and response required by the principles presented in PSR Ch. 3.
- NEDC-34192P, "BWRX-300 UK GDA Ch. 20: Environmental Aspects," (Reference 3-29) – presents the environmental aspects with consideration of the relevant principles presented in PSR Ch. 3.
- NEDC-34193P, "BWRX-300 UK GDA Ch. 21: Decommissioning and End of Life Aspects," (Reference 3-30) – presents codes and guidelines applied in decommissioning and end of life aspects based on the selection principles of codes and standards provided in PSR Ch. 3.
- NEDC-34194P, "BWRX-300 UK GDA Ch. 22: Structural Integrity," (Reference 3-31) – demonstrates the structural integrity by applying design requirements based on the relevant principles presented in PSR Ch. 3.
- NEDC-34195P, "BWRX-300 UK GDA Ch. 23: Reactor Chemistry," (Reference 3-32) – presents codes and guidelines applied in chemistry based on the selection principles of codes and standards provided in PSR Ch. 3.
- NEDC-34196P, BWRX-300 UK GDA Ch. 24: Conventional Safety and Fire Safety," (Reference 3-33) – presents the applicable codes and standards in conventional safety and fire safety which are compliant with the selection principles of codes and standards provided in PSR Ch. 3.
- NEDC-34197P, "BWRX-300 UK GDA Ch. 25: Security," (Reference 3-34) – describes the general approach to security as well as physical and cybersecurity with consideration of the principles presented in PSR Ch. 3.
- NEDC-34198P, "BWRX-300 UK GDA Ch. 26: Interim Storage of Spent Fuel," (Reference 3-35) – presents applicable codes and standards in interim storage of

spent fuel which are based on the selection principles of codes and standards presented in PSR Ch. 3.

- NEDC-34199P, “BWRX-300 UK GDA Ch. 27: ALARP Evaluation,” (Reference 3-36) – presents the ALARP evaluation to support and assess the achievement of the nuclear safety objective provided in PSR Ch. 3.
- NEDC-34200P, “BWRX-300 UK GDA Ch. 28: Safeguards,” (Reference 3-37) – demonstrates understanding of safeguards requirements at the generic level and how they are accommodated in the standard plant design, with consideration of the principles presented in PSR Ch. 3.

Claims and arguments relevant to GDA step 2 objectives and scope are summarised in Appendix A, along with an ALARP position. Appendix B provides a Forward Action Plan, which includes future work commitments and recommendations for future work where ‘gaps’ to GDA expectations have been identified. UK-specific context is provided in Appendix C, including UK Context for Numerical Targets which is presented in Section C.1, ALARP context which is presented in Section C.2, and the UK approach to Categorisation and Classification is discussed in Section C.3.

Baseline Design

The BWRX-300 baseline design has been developed and justified in part upon reference to US Nuclear Regulatory Commission (USNRC) guidance and is intended for deployment in the UK. As such, PSR Ch. 3 refers throughout to use of USNRC guidance. A Forward Action has been raised to consider alternative codes and standards and justify use as Regulatory Good Practice.

3.1. General Safety Design Basis

The overall safety philosophy for the design of the BWRX-300 is referred to as the Safety Strategy and presented in NEDC-33934P, “BWRX-300 Safety Strategy,” (Reference 3-38). The objective of the Safety Strategy is to establish a design with a high level of safety. This is accomplished through incorporation of design requirements based on the principles set forth in the International Atomic Energy Agency document SSR-2/1, “Safety of Nuclear Power Plants: Design,” (Reference 3-39).

The establishment of the BWRX-300 design basis is achieved through an iterative safety framework wherein the design is implemented to meet defined safety objectives and safety goals that are confirmed via deterministic and probabilistic safety analyses. Results of safety analyses then provide feedback into the design and the process is repeated as required until adequate design and regulatory safety margins are achieved.

3.1.1 Safety Objectives

The BWRX-300 design adopts the safety objectives established by the IAEA Safety Standards Series No. SF-1, “Fundamental Safety Principles,” (Reference 3-40) and documented in the International Nuclear Safety Advisory Group (INSAG) publication INSAG-12, “Basic Safety Principles for Nuclear Power Plants 75-INSAG-3,” (Reference 3-41) which when followed ensure that reactor facilities are operated, and activities conducted to achieve the highest standards of safety that can be reasonably achieved. These safety objectives are described below:

General Nuclear Safety Objective: To protect individuals, society, and the environment by establishing and maintaining in Nuclear Power Plants (NPPs) an effective defence against radiological hazard

The general nuclear safety objective is supported by the following complementary safety objectives:

- **Radiation Protection Objective**: To ensure in normal operation that radiation exposure within the plant and due to any release of radioactive material from the plant is As Low As Reasonably Achievable (ALARA), economic, and social factors being taken into account, and below prescribed limits, and to ensure mitigation of the extent of radiation exposure due to accidents.
- **Technical Safety Objective**: To prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small.

The high-level safety objectives inform the principal safety objectives in the design and safety analyses.

As Low As Reasonably Practicable

It is necessary to show that the risks to the workers and the public are ALARP. This requires that all reasonable measures are taken in the design, construction, and operation of the plant to minimize the radiation dose received by workers and public, unless such measures are grossly disproportionate to the risk avoided.

The ALARP methodology and evaluation are provided in NEDC-34199P (Reference 3-36).

Section C.2 of Appendix C presents further discussion on the legal basis for ALARP in the UK and the approach to ALARP that will be presented in this PSR.

3.1.2 Fundamental Safety Functions

NEDC-33934P (Reference 3-38) defines and maintains the Fundamental Safety Functions (FSFs) to ensure protection of the physical barriers. For a given event sequence, if the functional DLs required to fulfill the FSFs are performed successfully, then the corresponding barriers remain effective.

The design of the BWRX-300 fulfills FSFs at all plant states (defined in Section 3.1.5) which ensures the design meets its safety objectives. The FSFs for the BWRX-300 are:

- Control of reactivity
- Removal of heat from the fuel (in the reactor, during fuel storage and handling, and including long-term heat removal)
- Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental releases

The FSFs are defined in IAEA SSR-2/1 (Reference 3-39).

A systematic approach is taken to identify the FSFs and those SSCs necessary to fulfill the FSFs following a Postulated Initiating Event (PIE). The results of applying the systematic approach are gathered in the fault list, which provides traceability between DL functions with a direct role in fulfilling an FSF and the plant states and event sequences in which each of those functions performs that role.

Fulfillment of the FSFs prevent or mitigate radiological releases by ensuring the physical barriers to releases (fuel matrix, fuel cladding, Reactor Coolant Pressure Boundary (RCPB), and containment) remain effective. In addition to the protection of barriers, a means of monitoring the status of key plant parameters is provided for ensuring that the FSF are fulfilled. From this perspective, the monitoring function is treated as inherent to fulfillment of the FSFs. Other considerations for the monitoring function are as follows:

- If a manual operator action plays a role in performing an FSF, the monitoring function of the equipment used to display key plant parameters that are necessary for the operator to perform the manual action successfully are also considered part of the FSF.
- Certain monitoring functions allow the operator to confirm ongoing effectiveness of the FSFs during all plant states, to implement post-accident procedures, and to make decisions in support of emergency planning.
- Post-Accident Monitoring (PAM) is important for operator decision making such as taking manual actions and implementing functions. Therefore, the designation, treatment and display of certain plant parameters or measurements as post-accident monitoring variables is a supporting design feature.
- A minimum set of monitoring functions and display of parameters that do not support the operator actions are provided to support accident assessment.

Fulfillment of the FSFs is intrinsic to BWRX-300 Safety Strategy. A systematic approach is taken to identify the FSFs and those SSCs necessary to fulfill the FSFs following a PIE. This systematic approach is detailed in the D-in-D discussion in Section 3.1.7.

3.1.3 Radiation Protection and Radiological Acceptance Criteria

The BWRX-300 is designed to meet the Radiation Protection Objective by ensuring that potential radiation dose to workers and the public is kept below prescribed regulatory limits.

This is achieved by a comprehensive and appropriately conservative source term derivation identifying radiation sources during the design phase to ensure means are provided to reduce occupational exposure during plant operation, maintenance, and decommissioning.

Safety features and measures include:

- Passive engineered safety features
- Active engineered safety features
- Administrative safety measures

Engineered safety features include shielding, containment, ventilation, remote handling, and interlocks. Administrative safety measures that reduce exposure to the hazard during planned operations include restrictions on occupancy, monitoring arrangements, pre-planning of exposure and the use of barriers and notices. Passive engineered safety measures (e.g., containment or shielding) are preferred before active engineered safety features and administrative safety measures. Human factors considerations are incorporated into the engineered and administrative measures (See NEDC-34190P (Reference 3-27) for details).

System design evaluations are performed in parallel with other activities to ensure systems support operational objectives. These evaluations include the development of reasonable and practical measures to achieve minimal dose to workers and the public.

Details on how radiation protection is considered in the design for operational states and accident conditions are provided in NEDC-34175P (Reference 3-12).

NEDC-34178P, “BWRX-300 UK GDA Ch. 15: Safety Analysis (Including Fault Studies, PSA, and Hazard Assessment,” (Reference 3-15) describes the dose calculation methodology used in the deterministic safety analysis. Results of the analyses are summarized in NEDC-34187P, “BWRX-300 UK GDA Ch. 15.9: Safety Analysis: Summary of the Results of the Safety Analyses (Including Fault Schedule),” (Reference 3-24) demonstrating that the radiological consequences of the analysed events do not exceed the acceptance criteria for Anticipated Operational Occurrences (AOOs) and for DBAs.

3.1.4 Safety Goals

In addition to the dose acceptance criteria, PSA is used to assess risks posed by reactor facility operation through the application of quantitative safety goals. These include core damage frequency, and small and large release frequency.

Core damage frequency is a measure of the capability of the design to prevent an accident that leads to core damage. Small release frequency and large release frequency are measures of the plant's accident mitigation capabilities. They also represent measures of risk to society and to the environment due to the operation of reactor facilities.

For the BWRX-300 standard plant design these plant safety goals are presented in NEDC-33934P (Reference 3-38) and reproduced below:

- **Core damage frequency** - The sum of frequencies of all fault sequences that can lead to significant core degradation shall be less than 1E-6 per reactor-year
- **Large release frequency** - The sum of frequencies of all fault sequences that can lead to a release to the environment that requires long-term relocation of the local population shall be less than 1E-7 per reactor-year

The PSA is described in detail in NEDC-34184P, “BWRX-300 UK GDA Ch. 15.6: Safety Analysis: Probabilistic Safety Assessment,” (Reference 3-21).

Section Appendix C of Appendix C presents further discussion of these safety goals in the context of UK numerical targets for normal operational, design basis fault and radiological accident risks to people on and off the site.

3.1.5 Plant States Considered in the Design Basis

The range of conditions and events considered are categorised into plant states based on their frequency of occurrence. Plant states include operational states and accident conditions. Operational states included in the design basis are Normal Operation and AOOs. Accident conditions considered in the design basis are DBAs. Design Extension Conditions (DECs) are accident conditions considered in the design but are outside of the design basis based on their lower expected frequency of occurrence:

- Normal Operation includes the operational states that are expected to occur frequently or regularly during plant operation, including the following Normal Plant Operational Modes: Power Operation, Startup, Hot Shutdown, Stable Shutdown, Cold Shutdown, and Refuelling, maintenance, or manoeuvring of the plant (the normal plant operating modes are described in NEDC-34188P (Reference 3-25)).
- AOOs are deviations from normal operation that are expected to occur at least once during the operating lifetime of the reactor facility but that, with the appropriate design measures, do not cause any significant damage to SC components, or lead to accident conditions.
- Design Basis Accidents are conditions for which a reactor facility is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits.
- Design Extension Conditions are postulated accident conditions that are less frequent than DBAs. DECs are a subset of Beyond-Design-Basis Accidents (BDBAs), and are therefore, not part of the design basis. DECs are considered in the design process of the facility in accordance with best-estimate methodology DECs can occur without core damage or with core damage where releases of radioactive material are reasonably contained and kept within acceptable limits.

BDBAs other than DECs are accidents for which confinement of radioactive materials cannot be reasonably achieved. These are referred to as severe accidents and involve a catastrophic failure, core damage, and fission product release. A severe accident is generally considered to begin with the onset of core damage.

Representative DECs with core damage are postulated to provide inputs for the design of the containment and of the safety features ensuring containment functionality. This set of accidents is considered in the design of corresponding safety features for DECs and represents a set of representative cases that envelope other severe accidents with more limited degradation of the core.

These accidents scenarios are considered for practical elimination as described in Section 3.1.9.

Events are assigned to a plant state based on the expected frequency of the fault sequence, which includes a PIE and, in some cases, additional failures of mitigating functions. PIEs are the events that lead to deviations from normal operation. PIEs originate from operating errors, equipment failures, or internal or external hazard of natural or human origin.

Frequency ranges for plant states are:

- AOO (greater than 1E-02 per reactor-year)
- DBA (1E-02 to 1E-05 per reactor-year)
- DEC (less than 1E-05 per reactor-year)

The design requirements of SSCs are developed to ensure that the plant is capable of meeting applicable requirements for each plant state. This is demonstrated through safety analyses as described in NEDC-34178P (Reference 3-15).

The facility is operated, monitored, and maintained within safe operating configurations or is transitioned to a safe operating configuration in accordance with operating procedures that are consistent with the design (See NEDC-34176P Reference 3-13 for details).

Acceptance criteria are assigned to each plant state in the design, considering the principle that frequent fault sequences have only minor or no radiological consequences, and that any fault sequences that may result in severe consequences are of extremely low probability.

For normal operating modes, the Operating Limits and Conditions (OLCs) serve as acceptance criteria as they are the set of limits and conditions within which the facility must be operated to ensure it is operated safely. OLCs are established as discussed in NEDC-34188P (Reference 3-25).

For each AOO and DBA fault sequence, acceptance criteria are defined and met to confirm the effectiveness of plant systems in maintaining the integrity of physical barriers against releases of radioactive material. These acceptance criteria are discussed and summarized in NEDC-34181P, “BWRX-300 UK GDA Ch. 15.3: Safety Analysis: Safety Objective and Acceptance Criteria,” (Reference 3-18).

For DEC fault sequences, the safety objectives are to prevent significant core damage, mitigate accident consequences, and protect containment integrity. These objectives are demonstrated in PSA by showing that the plant meets the established safety goals (described in Section 3.1.3) (PSA is described in detail in NEDC-34178P, (Reference 3-15)). Also, it is demonstrated that procedures and equipment put in place to handle accident management needs are effective in responding to DECs. This is accomplished through the operating procedures described in NEDC-34176P (Reference 3-13) and through complementary design features described in NEDC-34178P (Reference 3-15).

The general approach to defining the design basis for the BWRX-300 involves establishing the plant states described above, identifying the PIEs leading to a deviation from normal operation and categorising mitigating functions based on their ability to prevent and mitigate the progression of events ensuring that the safety objectives are met.

3.1.6 Prevention and Mitigation of Accidents

The design of the BWRX-300 includes provisions to prevent and to mitigate the consequences of accidents and to ensure that the likelihood that an accident will have harmful consequences is extremely low.

The primary means of preventing and mitigating the consequences of accidents is through the application of D-in-D. The application of D-in-D for the BWRX-300 design is described below.

3.1.7 Defence-in-Depth

The implementation of D-in-D in the BWRX-300 design is the basis for the Safety Strategy for ensuring an adequate level of safety is achieved by the design.

BWRX-300 Defence-in-Depth Concept

The concept of D-in-D involves the provision of multiple layers of defence against some undesirable outcome rather than a single, strong defensive layer. In the case of a NPP, the undesirable outcome is the exposure of workers, the public or the environment to radioactivity exceeding levels determined to be safe.

There are two types of defensive layering considered:

1. Physical barriers in place to prevent the release of radioactivity: The fuel matrix, fuel cladding, RCPB, and containment. The integrity of one or more physical barriers must be maintained to prevent unacceptable releases.
2. A combination of active, passive, and inherent safety features used to minimize challenges to the physical barriers, to maintain the integrity of the barriers and, in case a barrier is breached, to ensure the integrity of the remaining barriers.

While the physical barriers themselves represent multiple layers of defence against radioactive releases, in the BWRX-300 D-in-D application, the physical barriers are not themselves referred to as “DLs”. That term is reserved for the layers of defence comprising features, functions and practices that protect the integrity of the barriers. The D-in-D concept applied is largely focused on identifying and organizing features, functions, and practices into DLs without explicit acknowledgment of the physical barriers. The fundamental purpose of the DLs is to ensure the integrity of the physical barriers by applying multiple levels of protection.

The BWRX-300 D-in-D concept uses the FSFs described above to define the interface between the DLs and the physical barriers. In a given plant scenario, if the FSFs are performed successfully, then the corresponding physical barriers remain effective.

Defence Lines

Five DLs (or levels), DL1 through Defence Line 5 (DL5), are adopted consistent with IAEA SSR-2/1 (Reference 3-39). Figure 3-1 illustrates the DLs as they correspond to the plant states.

The first DL1 does not include plant functions. It minimizes potential for PIEs to occur in the first place and minimizes potential for failures to occur in subsequent DLs by assuring high quality and conservatism in design, construction, and operation. The second, third, and fourth DLs (DL2, DL3, and DL4) comprise plant functions that act to prevent PIEs from leading to significant radioactive releases. The fifth DL5 involves off-site emergency preparedness to protect the public in case a substantial radioactive release occurs.

The DLs include measures such as engineering and operational practices, plant features, and plant functions. These measures are incorporated such that:

- The normal operation of the plant is monitored and controlled such that PIEs that lead to AOOs can be mitigated before evolving into DBAs.
- The consequences are limited if a DBA does develop.
- Multiple DLs are capable of independently performing the FSFs. While this means that more than one DL is capable of independently performing the FSFs for D-in-D, DL independence from all other DLs is based on how specific DLs are credited for specific fault sequences.

Table 3-1 provides a high-level description of the objective, and the design means and operational means for supporting the DLs. The following is a brief description of each of the DLs.

Defence Line 1

The purpose of the first level of defence is to prevent deviations from normal operation and the failure of important SSCs. This is achieved through the quality measures taken to minimize potential for failures and for initiating events to occur in the first place and to minimize potential for failures to occur in subsequent lines of defence. These quality measures cover the design, construction, inspections, operation, use of operational experience, periodic safety reviews, and maintenance and testing of the plant.

DL1 measures may support the basis for assumptions made in safety analyses. For example, the use of a high-quality design process and stringent equipment qualification for the most important components support the assumption that only a single failure is considered in the Conservative Deterministic Safety Analysis, discussed in NEDC-34183P, “BWRX-300 UK GDA Ch. 15.5: Safety Analysis: Deterministic Safety Analyses,” (Reference 3-20).

Examples of DL1 measures include:

- The clear definition of normal and abnormal operating conditions
- Maintenance and implementation of a quality assurance program consistent with nuclear regulations and industry standards
- Application of appropriate industry standards to the design of SSCs
- Adequate design margins
- Robust design processes including design verifications
- Comprehensive testing programs
- Provisions for adequate time for operators to respond to events and appropriate human machine interfaces, including operator aids, to reduce the burden on the operators
- Deterministic safety analyses including appropriate conservatism, supplemented by Probabilistic Safety Analysis to produce risk insights
- Categorisation and qualification of SSCs according to their safety significance
- Operational Limits and conditions
- Application of lessons learned through operating experience

Defence Line 2

The purpose of the second level of defence is to detect and control deviations from normal operational states to prevent AOOs from escalating to accident conditions. Functions that normally operate to maintain key reactor parameters (e.g., pressure, reactor level, and reactivity) within normal ranges are part of Defence Line 2 (DL2).

Examples of DL2 measures include:

- Anticipatory plant trips
- Maintain target power
- Maintain target level
- Maintain target pressure
- Control Rod Block

Defence Line 3

For the third level of defence, it is assumed that, although very unlikely, the escalation of certain AOO or DBA PIEs might not be controlled at a preceding level and that an accident

could develop. In the design of the plant, such accidents are postulated to occur. Defence Line 3 (DL3) contains plant functions that act to mitigate a PIE by preventing fuel damage, when possible, which assures the integrity of the release barriers are maintained, and the plant is maintained in a safe state until normal operations are resumed.

The systems and equipment involved in performance of DL3 functions are designed for high reliability. Examples include eliminating the need for active support systems such as power supplies, ventilation, or cooling water, and minimizing the need for active control functions such as pumps and actively controlled valves.

The DL3 functions and equipment performing those functions are subject to functional and design requirements derived from the Conservative Deterministic Safety Analysis as described in NEDC-34183P (Reference 3-20).

Examples of DL3 measures include:

- Reactor Scram
- Isolation Condenser Initiation
- Main Steam Isolation
- Containment Isolation
- Reactor Pressure Vessel (RPV) Isolation

Defence Line 4

The purpose of the fourth level of defence is to mitigate DECs.

For the BWRX-300, Defence Line 4 (DL4) is comprised of two subsets of functions that are designated as Defence Line 4a (DL4a) and Defence Line 4b (DL4b) functions. DL4a functions mitigate DECs that occur without core damage. DECs progressing to core damage are mitigated by DL4b functions.

DL4a

DL4a functions are those that place and maintain the plant in a safe state in scenarios involving:

- DBAs sequences combined with multiple failures that prevent the DL3 SSCs from performing their intended function (i.e., Common Cause Failure (CCF) which is a failure of two or more SSCs due to a single specific event or cause).
- DEC PIEs considered as credible events that may involve multiple failures causing the loss of a FSF to be fulfilled as part of normal operation.

Examples of DL4a measures include:

- Diverse means of achieving the FSFs that are independent of and diverse from the SSCs carrying out the DL3 functions that are presumed to have failed.
- Scrams initiated by the Diverse Protection System.

DL4b

DL4b includes:

- Functions provided in scenarios leading to core damage to limit the radiological releases in case of core damage and are aimed at maintaining the containment functions for extreme events, multiple events, or multiple failures that defeat DL2, DL3, and DL4a.

- Functions provided to mitigate the effects from a damaged core and to preserve the FSF of confinement of radioactive material while limiting radioactive releases to acceptable levels.
- Safety features designated for DECs with core damage may, if practicable and available, also be used for preventing or minimizing significant core damage if it can be demonstrated that such use will not undermine the ability of these systems to perform their primary functions if conditions evolve into a severe accident.

Examples of DL4b measures include:

- DL4b measures carried out by complementary design features such as diverse and flexible equipment and portable components such as, portable uninterruptible power supplies and portable pumps
- Containment venting and overpressure protection
- Boron injection

A list of complementary design features is provided in NEDC-34178P (Reference 3-15).

Defence Line 5

The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents.

Defence Line 5 (DL5) includes emergency preparedness measures to cope with potential unacceptable releases in case the first four DLs are not effective. These are largely off-site measures taken to protect the public in a scenario involving substantial release of radiation.

Examples of DL5 measures:

- Severe accident management procedures
- Emergency response procedures and equipment (peripheral systems such as meteorological monitoring)
- On/off-site emergency response facilities, and certain communication systems may play a role in DL5). NEDC-34191P (Reference 3-28) discusses emergency response arrangements such as procedures and facilities. Communication systems are discussed in NEDC-34171P (Reference 3-8) (note that these measures may be initiated earlier in an event prior to progression to a severe accident).

Defence Line Independence

The BWRX-300 design incorporates independence in the application of D-in-D. DLs that mitigate the same event are independent as far as is practicable to avoid the failure of one level reducing the effectiveness of other levels. Some examples include:

- Among DL2, DL3 and DL4a, at least one DL can mitigate a PIE caused by or concurrent with a CCF in another DL, with the mitigation means being independent from the effects of the initiating CCF.
- All PIEs with a frequency greater than 1E-05 per reactor year caused by a single failure can be mitigated by DL3 and independently by DL2, DL4a, or a combination of DL2 and DL4a functions that are unaffected by the PIE. To the extent practicable, DL3 functions are independent and diverse from those in DL2 and from those in DL4a. This is because DL3 functions provide a backup to DL2 functions, and DL4a functions provide a backup to DL3 functions but DL4a functions are not needed to provide a direct backup to DL2 functions to maintain D-in-D for the same event.

- The DL4b functions intended for mitigating DECs are functionally and physically separated from the systems intended for other DL functions.
- DL4b features specifically designed to mitigate the consequences of accidents with core damage are independent from systems used in normal operation or used to mitigate AOOs as far as is practicable and with exceptions justified.
- Exceptions to rules of independence are described, assessed, and justified. If equipment supports functions in more than one DL, there is an increased focus on their reliability in the application of DL1 compared to a design feature credited in only one DL.

Safety Strategy Process for Implementing Defence-in-Depth

The BWRX-300 Safety Strategy implements the D-in-D concept into the design through evaluations and analyses as shown in Figure 3-2. These include:

- Hazard Evaluations
- Fault Evaluation
- Deterministic Safety Analyses
- PSA

The elements of Figure 3-2 are briefly described below.

Hazard Evaluations

The first step is to identify PIEs using a systematic methodology considering both direct and indirect events through hazard evaluations. The BWRX-300 Safety Strategy includes the following four types of hazard evaluations which are summarized in NEDC-34179P, “BWRX-300 UK GDA Ch. 15.1: Safety Analysis: General Considerations,” (Reference 3-16):

- Functional Failure Hazard Evaluation – assessment of failures of SSCs
- External Hazard Evaluation - assessment of external events such as earthquakes or aircraft crashes that have the potential to impact plant safety
- Internal Hazard Evaluation – assessment of hazards originating within the facility such as missiles from rotating equipment, fires, collapse of structures
- Human Operation Hazard Evaluation – human errors which could reasonably be expected to occur based on industry operating experience

The output of the four hazard evaluations are the potential PIEs for consideration in the Fault Evaluation.

Fault Evaluation

The Fault Evaluation process evaluates the PIEs determined as a result of the hazard analyses. PIEs are selected and organized along with fault sequences. As used herein, a fault is essentially a failure or a hazard and could be the initiator for or result from a PIE. A PIE is an event that initiates a fault sequence. A fault sequence consists of a PIE, and responses by mitigation functions (including both failed responses and successful responses).

The Fault Evaluation establishes traceability between the plant design and the safety analysis bases. The Fault Evaluation process including the selection and categorisation of PIEs and fault sequences for deterministic safety analysis is described in NEDC-34180P, “BWRX-300 UK GDA Ch. 15.2: Safety Analysis: ID, Categorisation and Grouping of PIEs and Accident Scenarios,” (Reference 3-17).

Deterministic Safety Analyses

The objective of deterministic safety analysis for NPPs is to confirm that:

- FSFs can be performed
- SSCs performing the FSF are designed with adequate margins
- physical barriers to radioactive release maintain their integrity as required

Deterministic safety analysis is supplemented by insights obtained from fabrication, testing, inspection, operating experience, and PSA. It demonstrates that the source term and the potential radiological consequences of different plant states are acceptable. It also demonstrates that the possibility of certain conditions arising that could lead to an early or a large radioactive release can be considered as “practically eliminated.”

The output of the Fault Evaluation process which includes the selection of PIEs and fault sequences organized by frequency are analysed in deterministic safety analysis. NEDC-34183P (Reference 3-20) provides more detail on the deterministic safety analysis process.

Probabilistic Safety Analyses

PSA are performed to understand the overall risk presented by the facility and to allow comparisons to be made against safety goals (defined in Section 3.1.3 – Safety Goals) They also provide essential understanding of strengths and weaknesses of a design with complex systems and interdependencies. They are used for evaluating complementary design feature concepts or changes in operating conditions and have many other applications to enhance safety decision.

To supplement quantitative PSA results, a severe accident analysis is performed to understand the complex physical phenomena associated with a reactor core damage scenario. This analysis supports confirmation that the radioactive release sequences modelled in the Level 2 PSA adequately reflect associated phenomena.

Severe accident analyses are used to complement the design deterministic safety and PSA in situations where the consequence is large, even if the calculated risks are low and/or the deterministic safety analysis provides a robust demonstration of fault tolerance. The severe accident analysis is not considered standalone piece of analysis deriving scenarios from first principles, but instead builds upon other types of analysis to create an overall safety case that is adequate in its coverage.

Detailed discussion of PSA and Severe Accident Analysis is provided in NEDC-34184P (Reference 3-21).

3.1.8 Application of General Design Requirements and Technical Acceptance Criteria

Deterministic Design Principles in Codes and Standards

A fundamental aspect of the BWRX-300 Safety Strategy is that the overall plant design applies good engineering practices for design, construction, operation, maintenance, and testing which relates to conformance to regulatory requirements, as well as industry codes and standards and norms for achieving high dependability in performance.

Engineering design rules are established and applied, as appropriate by the specific design discipline based on relevant codes, standards, and proven engineering practices.

Because codes or standards for the different design disciplines (e.g., mechanical, civil, and electrical) are not always based on compatible safety criteria, consistent acceptance criteria are established, and good engineering practices are used, to provide consistency in the

application of selected codes and standards in design. Analyses and evaluation of the codes and standards to be applied in the design, fabrication and construction of the plant is performed. The results of this analysis and evaluation are documented as part of the management system.

The plant architecture and systems design specifications demonstrate that the plant and the SSCs are designed, implemented, constructed, installed, operated, and maintained safely with respect to their application and maintenance of these guiding fundamental design principles that follow. Additionally, changes are performed using the same guiding fundamental design principles, using the same or better methods and processes to avoid compromising safety.

Minimise Probability of Structures, Systems and Components Failure

The probability of failure of systems and equipment is minimised through a design which provides predictable and repeatable performance of the FSFs. This is achieved by deploying highly reliable and dependable SSCs.

DL3 systems and equipment are designed to fail to a safe state or to a known, defined state to ensure safety is not jeopardised. Thus, reactor trip systems fail to the safe state, but engineered safety features systems may fail-safe or are non-actuated (e.g., isolation condenser cooling function). Fail-safe design is achieved through systematic identification of failure modes through Failure Modes and Effects Analyses (FMEA).

Systems are required to be testable to provide assurance of continued operability and availability when required. System maintainability is a fundamental aspect of the design, extending down to software by ensuring documented, well-designed, understandable code.

Integration of software into the overall system development process is a fundamental aspect of minimising failure probability. The Instrumentation and Control (I&C) System Life Cycle is applied to each I&C system which follows the overall lifecycle presented in International Electrotechnical Commission (IEC) 61513, “Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems,” (Reference 3-42). Further details on this process are provided in NEDC-34169P (Reference 3-6), 006N2631, “I&C Plant Level Design Assurance Plan,” (Reference 3-43), and 006N9508, “BWRX-300 Program Configuration Management Implementation Plan,” (Reference 3-44).

NEDC-34176P (Reference 3-13) describes how fitness for service is addressed in established programs that include: Reliability, Maintenance, Aging Management, Chemistry Control, Periodic and Inservice Inspections (ISIs). Programmatic requirements addressing fitness for service span the full life cycle of the facility beginning with inclusion in facility design decision making.

Independence

The most plausible reason for the failure of FSFs is the occurrence of dependent failures. Dependent failures are identified, and where practicable, measures are implemented in design, construction, and operation to eliminate the dependencies or reduce their potential effect. The application of independence is used in the Safety Strategy to enhance reliability and reduce potential for dependent failures. Independence is an essential aspect of effectiveness in the implementation of D-in-D.

The determination of independence of SSCs required to mitigate the consequences of a single or a likely combination of internal or external hazards on the plant is conducted through the Fault Evaluation introduced in Section 3.1.7 (Safety Strategy Process for Implementing D-in-D) and described in more detail in NEDC-34180P (Reference 3-17) and confirmed via the PSA in NEDC-34184P (Reference 3-21).

The PSA is also used to confirm the adequacy of the independence measures.

Independence is achieved by addressing the main causes of CCFs: functional, spatial, inherent, and human error dependencies as discussed in Section 3.1.8 (Single Failure Criterion).

Diversity

Diversity is the provision of dissimilar means of achieving the same objective. Diversity involves the use of design features which differ in the physical means of achieving a specific objective or use of different equipment made by different manufacturers. Diversity is achieved by incorporating different attributes into the systems or components. Such attributes could be different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers, for example. It is necessary to ensure that the diversity attribute achieves the desired increase in reliability in the as-built design. For example, to reduce the potential for CCFs the designer should examine the application of diversity for any similarity in materials, components and manufacturing processes, or subtle similarities in operating principles or common support features. If diverse systems or components are used, there is a consideration that reasonable assurance that such additions are of overall benefit, including consideration of the associated disadvantages such as the increased operational complication, additional maintenance and test procedures, and the potential for lower reliability.

Diversity is considered for digital equipment and active mechanical/electrical equipment. Diversity is not included for passive equipment such as pipes and tanks. Diversity is a DL1 provision used to strengthen subsequent DLs.

Separation

Functional isolation is used to reduce the likelihood of adverse interactions between equipment and components resulting from normal or abnormal operation or failure of any component in the systems. For example, in a power supply, functional isolation is commonly achieved using fuses and circuit breakers.

Separation supports DL function independence discussed in Section 3.1.7 (DL Independence). System layout and design uses physical separation to increase assurance that independence will be achieved, to preclude certain CCFs.

- Physical separation includes separation by geometry (such as distance or orientation); barriers; or a combination of these. The choice of the means of separation will depend on the PIEs considered in the design basis, such as the effects of fire, chemical explosion, aircraft crash, missile impact, flooding, extreme temperature, or humidity.
- In a redundant system and despite diverse provisions, the threat of CCFs from hazards such as fire may be reduced by system segregation. Segregation is the separation of components by distance or physical barriers. An example is the use of fire barriers to indicate individual fire zones, which may also serve as barriers to other hazards.
- Plant barriers that provide protection against certain faults or hazards are assessed to ensure that the barriers remain operable and accessible in the event of those faults or hazards occurring. This is particularly important where SSCs that perform DL functions are co-located with other plant equipment that do not.

Redundancy

Redundancy is the provision of more than the minimum number of nominally identical equipment items required to perform a specific safety function. Such redundant provisions allow a safety function to be satisfied when one or more systems or components (but not all) are unavailable, due to a variety of unspecified potential failure mechanisms or maintenance (e.g., identified faults or hazards). Redundancy enables failure or unavailability of at least one set of systems or components without loss of the function. For example, three or four pumps

may be provided for a particular function when any two would be capable of carrying it out. For the purposes of redundancy, identical or diverse components may be used.

The application of independence, diversity, separation, and redundancy in the design is described in each system design description.

Single Failure Criterion

The BWRX-300 design addresses the single failure criterion through design and safety analyses to ensure reliability of DL3 functions. DL3 functions are considered as they are within the design basis. Each safety group (DL3 function) is assessed for capability in fulfilling its required function even if a failure of a single component occurs within this group.

A single failure is one which results in the loss of capability of a single system or component to perform its intended DL3 function(s), and any consequential failure(s) which result from it.

For the BWRX-300, the single failure criterion is considered in two ways:

1. As a design attribute that is typically achieved through redundancy in the system architecture of the SSCs carrying out DL3 functions. This involves a systematic search for potential single failure points and their effects on prescribed missions (i.e., FMEA).
2. As an assumption made in the conservative deterministic safety analysis, in addition to the PIE and any additional failures, all identifiable undetectable faults are included to demonstrate a high degree of confidence that acceptance criteria will be met.

During the design process, systems that are designed to carry out a DL3 function must be capable of carrying out their mission despite the failure of any single component within the system or in an associated system that supports its operation. Design measures for ensuring high reliability of SSCs carrying out DL3 functions include incorporating independence, diversity, and redundancy (e.g., N+2 for a Class 1 Standby System), and also through the incorporation of passive and fail-safe features.

The PSA is used for identifying single failures for consideration in the deterministic safety analysis and is also a complementary means of demonstrating the insensitivity to single failures.

Common Cause Failures

Background Information and General Approach

CCFs are functional failures of multiple components due to a single specific event or cause. Such failures may affect several different Safety Class (SC) components simultaneously or may affect multiple components of the same type at the same time.

The event or cause of CCFs may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human induced event or an unintended cascading effect from any other operation or failure within the plant. Appropriate measures to minimise the effects of CCFs, such as the application of redundancy, diversity, and independence, are taken as far as practicable in the design.

Multiple failures can occur due to common weaknesses or dependencies shared by components. Such failures can cause failure of all redundant components in a single protection system or failure of components in more than one system. Dependent failures can considerably reduce the reliability of the protection systems relative to that expected from consideration of random failure mechanisms occurring in isolation. Identification of dependent failures is assessment by Functional Failure Hazards Evaluations.

The main types of failure dependencies that can cause a potential loss of safety function are as follows:

- Functional Dependencies, which arise from shared or common functional features such as a common electrical power source, a common cooling water system or a shared process fluid.
- Spatial Dependencies, which arise from physical features shared by components located in a common location such as common radiation or chemical conditions, a common environment and common support structures, and vulnerability to leaks of dangerous fluids (high temperature, corrosive or toxic).
- Inherent Dependencies, which arise from shared characteristics such as a common principle of operation or technical embodiment and a common failure mechanism such as mechanical overload or overpressure.
- Human Error Related Dependencies, which arise from human errors affecting some shared or common human process such as human error in design or manufacture, or operating staff error during operation and maintenance.

The general protective approach used for addressing postulated vulnerabilities to CCFs is diversity in the design. Dissimilarities in technology, function, implementation, and so forth, can mitigate the potential for common faults. The diversity approach to ensuring safety uses different (e.g., dissimilar) means to accomplish the same or equivalent function to compensate for a CCF that disables one or more levels of defence. Diversity is complementary to the principle of D-in-D, and it increases the chances that a DL function will be available when needed. Different DLs that mitigate the same event are diverse from each other to the extent practicable.

Another means of protecting against CCF is through feedback from operating experience that could identify weaknesses in the design, construction, operation and testing of equipment. In addition, conducting periodic inspection, surveillance, and testing provides opportunities to detect degradation or common causes before failures of SSCs. Quality assurance and quality control measures applied to SSCs commensurate with their importance help reduce preclude potential CCFs.

Common Cause Failures of Digital Instrumentation and Control Software

The BWRX-300 approach to assessment of CCF of Digital I&C software is through a consequence-based approach.

Even when functional dependencies are addressed through rigorous design and application of codes and standards, operating experience shows that software CCFs occur. Validating assumptions and modelling of software CCF modes can be challenging due to uncertainty as each Digital I&C system is unique, and extrapolation of failure data from one system to another may not be meaningful making the identification of failure scenarios difficult. Analysing each postulated CCF scenario is not practicable; therefore, using a consequence-based approach can limit the number of CCF scenarios is considered. This approach considers the radiological or dose consequences that could result due to CCFs in the software.

Defence Line Approach to Common Cause Failure

A multi-pronged approach and the systematic integration of CCFs in DL functions, both as PIEs and as failures affecting fault sequence mitigation, are applied in deterministic safety analyses for prevention and mitigation in the D-in-D approach. Examples include:

- DL3 systems and functions are designed and rigorously qualified to be resistant to the effects of environments that could cause common failures, including DBA environments.

- For internal and external events resulting in DECs, the design includes independent and diverse system functions to cope with the effects of CCF (e.g., DL4a).
- Diverse accident monitoring instrumentation for severe accident management (e.g., DL4b) is provided.

The D-in-D approach is designed to include analyses of a reasonable set of CCF scenarios to provide assurance that the plant is protected against CCF phenomena. This approach is implemented using a set of CCF application guidelines to define the CCF modes that are included, how the failure modes are applied, and which assumptions can be made regarding equipment operability.

Other Approaches for Ensuring Safety

In addition to the design principles discussed above, the BWRX-300 design incorporates the following approaches to ensure safety.

Simplicity in Design

An implicit approach to reliability is to deploy the design with minimal complexity, with the knowledge that complexity may be required to enhance reliability or reduce the potential for human error. Where complexity is required (e.g., self-diagnostics, redundancy within the equipment in a single division), the complexity is documented and justified as necessary and appropriate for enhancing reliability, surveillance, calibration, and other required system or equipment attributes. There are tradeoffs in complexity, such as increasing the complexity by designing the system to reduce the human actions necessary for surveillance which also decreases the potential for human error, which enhances system reliability.

The BWRX-300 is specifically designed to enhance safety through simplification and reducing its dependence on human intervention. This is achieved through increasing its reliance on natural circulation and natural phenomena-driven safety systems (these are passive features as discussed below). These safety enhancements, in combination with its reduction in scale and complexity including a reduction in total number of active SSCs, simplifies operations and maintenance.

Passive Safety Features

The design of the BWRX-300 uses passive functions that do not require external sources of power or operator actions. DL3 functions are passive to the extent that is practicable and, therefore, have significantly less reliance on supporting systems or operator actions.

Examples of the BWRX-300 passive design features include:

- Safety Class 1 (SC1) batteries are capable of powering loads for a minimum of 72 hours. The design ensures that plant safety is maintained even after battery depletion.
- The BWRX-300 design utilises passive natural circulation for fuel cooling and containment heat removal. The plant is designed with the capability to cope with decay heat for seven days using only installed systems with no reliance on significant operator actions or external resources.

The mitigation of loss-of-coolant accidents is built on utilisation of inherent margins (e.g., larger water inventory) to eliminate system challenges, reduced number, and size of RPV nozzles as compared to predecessor designs, and elimination of fluid system nozzles located below a level well above the top of active fuel to conserve inventory. The relatively large reactor pressure volume of the relatively tall chimney region provides a substantial reservoir of water above the core. This ensures the core remains covered following fault sequences involving feedwater flow interruptions or loss-of-coolant accidents without the need for active components (such as pumps). Additionally, the RPV is equipped with isolation valves attached

directly to the reactor vessel for large bore piping systems to preserve reactor coolant inventory ensuring that adequate core cooling is maintained.

The application of these design concepts is described in each system design description.

Radiological Protection Principles

Administrative programs and procedures, in conjunction with facility design, ensure that occupational radiation exposure to personnel is kept ALARP. The systematic application of the ALARP principle during the design phase of the BWRX-300 establishes the basic design criteria observed to reducing occupational exposure during plant operation and maintenance, decommissioning and post-accident ALARP.

ALARP design requirements are established to improve the layout of enclosures, accesses, and exits from controlled areas of the plant structures that confine radioactive material. The design of plant SSCs minimizes personnel exposure to radiation during operation, inspection, maintenance, or plant design modifications.

The ALARP design requirements keep radiation exposures ALARP during normal operation or AOOs and planned radioactive material releases below regulatory limits. The ALARP design criteria includes provisions for mitigating the radiological consequences of design basis accidents.

The BWRX-300 plant design:

- Precludes the release of radioactive material to the public and the environment that exceeds the limits of applicable regulations for normal operations, transients, and accidents
- Minimises personnel exposure
- Minimises the generation of radioactive contamination and waste

The following BWRX-300 design features minimise radioactive contamination:

- Containment in areas where leaks and spills are likely to occur
- Leak detection capability to provide prompt SSCs leakage
- Usage of leak detection methods (e.g., instrumentation, automated samplers) capable of early leak detection in areas difficult (inaccessible) to conduct regular inspections (such as the fuel pool), and buried, embedded or subterranean piping) to avoid release of contamination. All BWRX-300 tanks containing radioactive fluids are within the Radwaste Building that have cubicles and drain back into the radioactive liquid waste for processing.
- Minimizing embedded piping, sumps, or buried equipment to facilitate decommissioning
- Removal or replacement of equipment or components during facility operation or decommissioning
- Minimizes the generation of radioactive contamination and waste during operation decommissioning by reducing the volume of components and structures that become contaminated during plant operation

Design for Decommissioning Principles

Operational Experience (OPEX) demonstrates that decommissioning of reactor facilities is best facilitated if considered during the design phase. Assessment of future facility decommissioning and dismantling activities at the design phase include consideration of OPEX gained from the decommissioning of existing facilities, as well as those facilities that

are in long-term safe storage. The consideration of decommissioning at the design phase is expected to result in lower worker doses, reduced environmental impacts, and improved life cycle management of the facility.

BWRX-300 design features to facilitate decommissioning include:

- Optimised for constructability, which may be beneficial for dismantling the facility during decommissioning
- Modularisation which will provide guidance in selection of disassembly methods employed during decommissioning
- Maintaining low occupational exposures
- Provisions for draining, flushing, and decontaminating equipment and piping
- Design of equipment to minimise the buildup of radioactive material and to facilitate flushing of piping systems
- Separation of more highly radioactive equipment from less radioactive equipment

NEDC-34193P (Reference 3-30) provides further details on design for decommissioning.

Technical Acceptance Criteria

To meet the radiological acceptance criteria, derived accepted criteria are defined for the fuel pellet, fuel cladding, RCPB and containment. Deterministic safety analyses are performed to demonstrate that these criteria have been met. A description of acceptance criteria is provided in NEDC-34181P (Reference 3-18). Details of the deterministic safety analysis are presented in NEDC-34178P (Reference 3-15).

3.1.9 Practical Elimination

Consistent with IAEA SSR-2/1 (Reference 3-39), the BWRX-300 design is such that fault sequences that could lead to an early or large radioactive release are practically eliminated.

The definition of early and large radioactive release (from IAEA SSR-2/1) (Reference 3-39) in this context are:

1. An early radioactive release is a release of radioactive material for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time
2. A large radioactive release is a release of radioactive material for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment

Fault sequences with early or large releases could be considered to have been practically eliminated if either of the following apply:

- It is physically impossible for the accident sequence to occur
- The fault sequence can be considered with a high degree of confidence to be extremely unlikely to arise

Practical elimination is considered to refer only to those fault sequences leading to or involving core damage (e.g., a severe accident) for which the confinement of radioactive materials cannot be reasonably achieved.

The aim of the practical elimination concept is to reinforce D-in-D by focused analysis of those conditions having the potential for early radioactive release or a large radioactive release.

The justification of practical elimination preferably relies on a demonstration of physical impossibility for the accident sequence to occur. If this is not achievable, a demonstration of

an extremely low likelihood of occurrence with a high level of confidence is provided. Sufficiently robust arguments and evidence are used to demonstrate the reliability of the lines of defence. If additional features are identified that prevent accidents or mitigation accident consequences, these features are considered for implementation as far as practicable.

The set of individual fault sequences that might lead to an early radioactive release or a large radioactive release are grouped to form a limited number of representative cases or type of accident conditions.

Severe accident phenomena based on operating experience with predecessor advanced Light Water Reactors (LWRs) serve as a starting point for consideration for practical elimination. Analyses demonstrating practical elimination are described in NEDC-34178P (Reference 3-15).

3.1.10 Safety Margins and Avoidance of Cliff-Edge Effects

A cliff-edge effect is described as a small change of conditions that may lead to a significant increase in the severity of consequences.

In the BWRX-300 Safety Strategy, the principle of multiple physical barriers to the release of radioactive material and protection of those barriers is incorporated in the design as a DL1 measure. Margins are incorporated into the design of the physical barriers to demonstrate their capability in postulated scenarios that are more severe (by a small amount) than those in the design basis without incurring cliff-edge effects.

Conservative safety margins and sensitivity analyses are applied in safety analyses to account for assumptions and uncertainties. Additional details on the application of safety margins in Deterministic Safety Analysis are described in NEDC-34183P (Reference 3-20). As part of the PSA, sensitivity and uncertainty analysis is conducted to demonstrate consideration of potential cliff-edge effects (See PSR Ch. 15.6, Reference 3-21).

3.1.11 Design Approaches for the Reactor Core and for Fuel Storage

Design Approach for Reactor Core

The reactor core is designed to maintain the integrity of the fuel and the fuel cladding. The fundamental safety functions of control of reactivity, removal of heat from the reactor and fuel, and confinement of radioactive materials are inherent design features for the reactor core.

The reactor core, the fuel, and fuel assemblies, including fuel channels and control blades, are designed such that the reactor can be shut down, cooled, and held subcritical with adequate margin in operational states, DBAs, and DECs. Reactivity control ensures shutdown margin for shutdown states and any credible changes in core configuration. The design ensures that the fission chain reaction is controlled during operational states. The design limits positive reactivity through inherent neutronic and thermal-hydraulic characteristics, means of shutdown, and control to protect the reactor pressure boundary and prevent fuel damage.

The reactor core (including associated structures and cooling systems) is designed to withstand static and dynamic loading and vibration, to be compatible with expected chemicals, and to meet thermal material and radiation damage limits.

The reactor core design also provides for certain operator actions in accident scenarios to maintain the reactor in a shutdown condition, such as actions that might be addressed in emergency operating procedures or severe accident management guidelines.

Design Approach for Fuel Handling and Storage

The design of fuel handling and storage systems is consistent with the D-in-D approach applied to the reactor core with slightly different fundamental safety functions.

The design approach is to identify fuel handling and storage SSCs that are necessary to fulfil the following fundamental safety functions for all plant states:

- Maintaining subcriticality of the fuel
- Removal of the decay heat from irradiated fuel
- Confinement of radioactive material, shielding against radiation as well as limitation of accidental radioactive releases

The Safety Strategy principle for fuel handling and storage is to leverage design and safety features in relation to fuel handling and storage that have been proven either in predecessor BWR applications or are based on operating experience.

Subcriticality is maintained by preventing criticality through use of geometrically safe configurations. The design of fuel storage systems considers the use of physical means or physical processes to increase subcriticality margins in normal operation to avoid reaching criticality during PIEs, including those PIEs arising from the effects of internal hazards and external hazards.

Fuel handling and storage systems are designed to maintain adequate fuel cooling capabilities for irradiated fuel ensuring that the fuel cladding temperature limits and/or the coolant temperature limits, as defined for operational states and accident conditions, are not exceeded.

The fuel storage and handling, radioactive waste, and other systems that may contain radioactivity are designed to assure adequate safety under normal and postulated accident conditions. These systems are designed:

- With a capability to permit appropriate periodic inspection and testing of components safety features
- With suitable shielding for radiation protection
- With appropriate containment, confinement, and filtering systems
- With a residual heat removal capability having reliability and testability that reflects the importance to safety of decay heat and other residual heat removal
- To prevent significant reduction in fuel storage coolant inventory under accident conditions

Appropriate systems are provided in fuel storage and radioactive waste systems and associated handling areas:

- To detect conditions that may result in loss of residual heat removal capability and excessive radiation levels
- To initiate appropriate safety actions

Refer to NEDC-34171P (Reference 3-8) for a detailed description of the Fuel Handling and Storage Systems.

3.1.12 Consideration of Interactions Between Multiple Units

The scope of UK GDA is for a single unit. However, interactions between multiple units has been considered as detailed below.

Operating experience has demonstrated that interactions or shared equipment between multiple units can cause problems for the plant and for personnel. Lessons learned include:

- Significant interactions between multiple co-located radiological sources (e.g., reactor units, spent fuel pools, or dry fuel storage facilities) could result due to concurrent or consequential initiators.
- The timing of concurrent accident sequences involving multiple radiological sources on a site can challenge shared SSCs, as well as resources available for severe accident management and emergency response to the event.

Site evaluations would address multiple reactors or other co-located facilities and determine if these need to be treated as external hazards (e.g., external radiation sources) in the design of the BWRX-300.

Each BWRX-300 unit would have its own SC systems and its own safety features for DECs.

If multiple units are to be co-located, emergency planning and design and safety analyses, including consideration of CCFs in similarly design units, would demonstrate that sharing resources of equipment and personnel, including temporary equipment and emergency response personnel, would not be detrimental to plant operation, fuel storage, emergency planning, or accident management.

3.1.13 Design Considerations for Aging Management

Aging of SSCs is considered in the basic assumptions and in the input data to the safety, thermohydraulic and stress analyses. All system and component design specifications reference design requirements on aging, including those in the applicable codes and standards.

Aging and equipment qualification considerations are important aspects, complementary to each other in plant design. Equipment qualification is discussed in Section 3.9.

In designing components, system designers consider aging mechanisms and their effects on the safety, reliability, and performance of SSCs for those that are well known and understood. Additionally, system designers collect information from operations feedback, research and development, vendor recommendations, maintenance and operating manuals, and expert insight, and make design decisions based upon shared knowledge. For BWRX-300 there exists significant operating experience and insights regarding individual degradation mechanisms that have been considered in the aging management programs. For example, the United States Nuclear Regulatory Commission has developed a consistent approach to aging management in connection with license renewal for operating plants.

Known aging phenomena are quantified and considered in the design of SSCs. The design includes the effects of wear and all other known age-related degradation to ensure that safety and performance are maintained for the duration of their lifetime. If the component lifetime extends to the plant service life, as is the case for passive non-replaceable components, the design considers all normal and transitory operating conditions, including testing stressors, maintenance interventions and the consequences of plant and system outages. Analysed DBAs are considered as part of the operating life and hence part of the design calculations.

In general, margins consist of design margins, operational margins, and safety margins. They account for uncertainties, assumptions, instrument feedback tolerances and ranges, unexpected transitory peaks, contingencies, and operating flexibility. Margins are mainly set to minimize the probability of component failure. Only the unquantifiable aging effects are included in the margin estimates.

Design documents include as a minimum, the following aging management topics:

- A recommended strategy for aging management and prerequisites for its implementation
- Identification of SC SSCs in the plant that could be affected by aging.

- Proposals for appropriate materials monitoring and sampling programs, where aging may affect the capability of critical SSCs to perform their functions throughout the lifetime of the plant
- Appropriate consideration of operating experience with respect to aging
- Recommendations for aging management for SC SSCs (RB Diaphragm Plate Steel-Plate Composite (DP-SC) structures, mechanical components, electrical and instrumentation and control components, cables, etc.) and measures to monitor and mitigate their degradation
- Equipment qualification requirements of SC SSCs

General principles stating how the environment of structures, systems, and components are to be maintained within specified service conditions (location of ventilation, insulation of hot SSCs, radiation shielding, damping of vibrations, submerged conditions and water chemistry, selection of cable routes, etc.).

3.2. Categorisation of Functions and Classification of Structures, Systems and Components

The BWRX-300 approach to categorisation of functions and classifying SSCs is consistent with IAEA SSR-2/1 (Reference 3-39) and IAEA SSG-30, “Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” (Reference 3-45). Classification of SSCs is conducted to identify the importance of the SCC with respect to safety.

This section described how BWRX-300 SSCs are classified by:

- SC
- Seismic Category
- Quality Group

Classification of SSCs provides a means for applying appropriate design requirements and establishes a graded approach in the selection of materials, and application of codes and standards used in design, manufacturing, construction, testing and inspection of individual SSCs. Sections 3.6 through 3.9 in Attachment 1 of NEDC-34165P (Reference 3-1) describe the codes and standards applicable to civil, mechanical, I&C, and electrical SSCs based on classification.

The classification of SSCs also determines the degree of redundancy, diversity, separation, and reliability/availability required as described in Section 3.1.8. The requirement for Environmental Qualification (EQ) is based on the classification of SSCs as described in Section 3.9.3. In addition, SSCs classification informs procurement and quality assurance requirements as discussed in NEDC-34189P (Reference 3-26).

Section C.3 of Appendix C provides further discussion on the BWRX-300 approach to categorisation of functions and classifying SSCs in the context of UK expectations.

3.2.1 Safety Classification Background

The BWRX-300 approach to classifying SSCs is based primarily on deterministic methods and is directly traceable to the safety functions performed by the SSCs. This approach reflects:

- Consequences of the SSCs failure to perform its safety functions
- Expected frequency of the SSCs being called upon to perform its safety functions
- Time following a PIE at which, or the period for which, the SSCs may be called upon to perform a safety function

A fundamental element of the BWRX-300 SSCs classification approach is the direct correlation between the DL in which an SSCs performs a function, and the relative safety importance of that function.

Primary Function Categorisation

Section 4.2 of NEDC-33934P (Reference 3-38) provides a description of the process for assigning Safety Categories to Functions. This process is illustrated in NEDC-33934P, Table 4-1: Functional Safety Category Assignment NEDC-33934P (Reference 3-38), and identifies the SSCs functions that apply to each Safety Category for the following groups of functions:

- DL2 Functions (10^{-3} failures per demand) – Actively control key plant parameters associated with FSFs and detect and mitigate AOO PIEs
- DL3 Functions (10^{-2} failures per demand) – Detect and mitigate DBA PIEs and event sequences comprising AOO PIEs and failure of DL2 functions
- DL4a Functions – Detect and mitigate DECs, including event sequences associated with some DBA PIEs and failure of DL3 functions

- DL4b Functions – Detect and mitigate DECs to prevent core damage or mitigate the consequences of core damage events (severe accidents)
- Normal Functions – Functions typically operating during normal plant operation
- PAM Functions – Support monitoring and display of PAMs variables

Primary functions are those that directly perform the FSFs in support of DL2, DL3, DL4a or DL4b. Functions are categorised into three safety categories: Safety Category 1, Safety Category 2, and Safety Category 3, with Safety Category 1 being the most important. Safety Categories are applied to the primary functions as follows:

- Safety Category 1 is assigned to DL3 primary functions. DL3 functions assure the integrity of the barriers to release, place and maintain the plant in a safe state, and provide independence and diversity for all DL2 and DL4a functions caused by a single failure (and many CCFs). Accordingly, DL3 primary functions are the most important from a safety standpoint.
- Safety Category 2 is assigned to DL4a primary functions. Both DL2 and DL4a provide a redundant means to address PIEs (generally independent of DL3 functions) and are therefore important from a safety standpoint, although less important than DL3 functions. DL4a functions are a backup to DL3 functions, in the unlikely event a DL3 functions fails, and therefore have a higher consequence of failure than DL2 functions and are more important from a safety standpoint than DL2 functions.
- Safety Category 3 is assigned to DL2 and DL4b primary functions as they are the least important to safety. DL4b functions address severe accidents, which are extremely unlikely because failure of both DL3 and DL2 or DL4a functions would have to occur. Accordingly, DL4b functions are considered the least important to safety DL functions, despite the high consequence of failure.
- Non-Safety Category is assigned to all other functions.

In addition to categorising primary functions by the DL they support, function that provide a supporting role and functions that are not immediately required following a PIE are assigned to a Safety Category as described below and summarised in Table 3-2.

Integral Support Functions

Integral support functions are functions that support the primary function and are required to be performed concurrently with the primary function (e.g., a Heating, Ventilation, and Air Conditioning (HVAC) system maintaining the temperature of a space or area within an acceptable range during performance of the primary function (i.e., following the initiating event) to maintain equipment in an acceptable condition).

Integral support functions are considered part of the DL function (and therefore subject to DL function “rules,” such as independence and diversity) and are assigned the same safety category as the primary function they support.

Make-Ready Support Functions

Make-ready support functions are continuously available online functions that maintain the primary function, or a component required to perform the primary function, in a state of readiness but are not required to be performed at the time the primary function is performed. Make-ready functions must have monitoring, such that plant operators would be alerted if the make-ready support function were lost, or the readiness of the primary function or component were compromised. For example, maintaining the temperature of a pool of cooling water within

acceptable limits, with monitoring by pool temperature indication is an example of a make-ready support function.

Make-ready functions are not required at the time the primary function is performed and are not considered part of the DL function (and therefore not subject to DL function "rules," such as independence and diversity). The primary function would generally be considered unavailable if the make-ready function were compromised to the extent that the primary function might be compromised. Accordingly, make-ready functions are not required to be assigned the same safety category as the primary function. However, make-ready functions are important and are therefore assigned to safety categories as follows:

- Make-ready functions that support DL3 or DL4a functions are assigned to Safety Category 3
- All other make-ready functions can be assigned to Safety Category N

Delayed Functions

Delayed functions are primary or support functions that are not required to be performed until sometime after the initiating event. Because there would be ample time during the event to ensure these functions are available, delayed functions are not required to be assigned the same safety category as functions required immediately after the initiating event. If the function is not needed until after 72 hours into the event, it can be classified as Safety Category 2 (instead of Safety Category 1), and if the SSCs are not needed until after seven days into the event, it can be classified as Safety Category 3 (instead of Safety Category 1 or Safety Category 2). Delayed functions are not subject to DL function "rules," such as independence and diversity.

Normal Functions

Normal functions that perform a FSF during normal plant operation or that maintain key reactor parameters (e.g., reactor pressure and temperature) within normal ranges, and their integral support functions, are assigned to Safety Category 3. Make-ready functions for normal functions can be assigned to Safety Category N. If failure of a normal function would likely result in an initiating event that could challenge a FSF, the function should be assigned to Safety Category 3.

Assignment of Safety Class to Components

Safety Class is assigned to components based on the safety category of the functions they perform as follows:

- Safety Class 1 (SC1) is assigned to SSCs that perform a Safety Category 1 function
- Safety Class 2 (SC2) is assigned to SSCs that perform a Safety Category 2 function
- Safety Class 3 (SC3) is assigned to SSCs that perform a Safety Category 3 function
- Non-Safety Class (SCN) is assigned to all other SSCs

Just as with functions, a time-dependency is introduced for components that perform or support DL3 and DL4a functions. Specifically, if the component is not needed until after 72 hours into the event, it can be classified as SC2 (instead of SC1), and if the component is not needed until after seven days into the event, it can be classified as SC3 (instead of SC1 or SC2) because there would be ample time during the event to ensure those components are available.

Some component classifications are made for components that perform FSFs but may not be explicitly defined as part of a DL function. For example:

- Components that are part of design provisions that perform a FSF, whose failure is considered “practically eliminated,” are assigned to SC1. An example is the RPV.
- Components whose structural failure could damage the fission product barriers are assigned to SC1.
- Components that are part of the RCPB are assigned to SC1.
- Structures (excluding fuel handling equipment) are assigned a safety classification based on the highest safety classification of the components they house or support, excluding components whose failure, due to failure of the structure, results in fail-safe performance of the component’s safety category functions.

The safety classification of a system is the highest safety classification of any components within the system; however, the component safety classification, and not the system safety classification, defines the design rules applied to components. Assignment of safety classifications to systems is for convenience in understanding the relative importance of plant systems.

Not all components or parts of a system are necessarily assigned to the same SC as the system itself. For example, a process system may be classified as SC1 because one or more of its components support a DL3 function; however, the system may also contain components that support functions associated with other DLs or components that support no DL functions. These components are classified in accordance with the DL functions they support.

Structures are assigned a safety classification based on the highest safety classification of the components they house or support. Components whose failure, due to loss of functionality of the structure, would result in fail-safe performance of the component’s safety category function(s) need not be considered in the classification of the structure. The seismic categorisation of a building drives the design rules and performance requirements associated with preventing and mitigating the effects of external and internal hazards. Seismic categorisation methodology is described in Section 3.2.3.

3.2.2 Safety Classification Process

In alignment with IAEA guidance, this method of classifying the safety significance of SSCs is based primarily on deterministic methods because the DL functions are identified using deterministic safety analyses. The deterministic methods are complemented (where appropriate) by probabilistic methods and engineering judgment.

Design rules are then applied to systems and components based on their safety classification and the DL functions they support. Design bases for structures are derived from their seismic category. The safety classification process is iterative with the deterministic and probabilistic safety assessment and is maintained and updated throughout the design phase.

The following outlines the BWRX-300 classification process.

Review and Definition of PIEs – Hazard evaluations are performed (as introduced in Section 3.1.7 – Hazard Evaluations) to identify hazards with potential to challenge an FSF. The output of these hazard evaluations are potential PIEs.

Grouping and Identification of Representative PIEs – Potential PIEs are grouped by plant effect and occurrence frequency. Representative PIEs and fault sequences are selected for deterministic safety analyses as described in NEDC-34180P (Reference 3-17).

Identification of Plant-Specific Safety Functions to Prevent or Mitigate the PIEs – The deterministic safety analyses are performed and updated iteratively with design activities to

establish the plant-specific functions responsible for maintaining the FSFs during PIEs and fault sequences. The identification of plant-specific functions and their assignment to a DL is carried out in the Fault Evaluation described in NEDC-34180P (Reference 3-17) with traceability of each function to each PIE and PIE sequence in which it is credited.

Safety Categorisation of the Safety Functions – Assignment of a function designed to mitigate one or more PIEs to a DL reflects its relative importance to safety and its role in maintaining the FSFs under off-normal conditions. As such, each function receives a safety categorisation directly based on its assignment to a DL (as described in Section 3.2.1 above). The FSFs for the BWRX-300 are:

- Control of Reactivity
- Removal of heat from the fuel (in the reactor, during fuel storage and handling, and including long-term heat removal)
- Confinement of radioactive materials

Identification of SSCs that Provide the Safety Functions - Plant-level requirements are created for each DL function and decomposed into system-specific functional requirements to implement the credited DL functions, consistent with the plant performance modelled in the safety analyses. These requirements are then allocated to the applicable system design description which identifies the components that support the system DL functions.

Assignment of SSCs to a Safety Class Corresponding to the Safety Category - SC is assigned to SSCs based on the SSCs' safety category.

Verification of SSCs Classification - The deterministic safety analyses are maintained and updated as the plant design matures. Confirmation of SSCs classification is achieved when the deterministic safety analyses models reflect the final plant design and demonstrate compliance to the analysis acceptance criteria (which include rules governing how classified equipment can be credited in each analysis case). This verification is complemented, as appropriate, by insights from the PSA.

Identification of Engineering Design Rules for Classified SSCs - Engineering design rules are applied to SSCs based on several factors including their SC, their DL role, their status as a pressure boundary component, their role during and following earthquakes, and their operational environment. The design rules establish the scope of codes and standards applied to an SSCs, as well as requirements for reliability, diversity, redundancy, and independence applicable to an SSCs. These design rules are discussed in Section 3.1.8.

3.2.3 Seismic Categories

Seismic Category reflects SSCs requirements during and after a seismic event and governs how the SSCs is seismically designed and qualified. BWRX-300 Seismic Category is assigned as follows:

- **Seismic Category 1A or 1B** – SSCs that are required to remain functional during and after a seismic event are considered Category 1A or 1B:
  - Seismic Category 1A for passive structures and components that are required to remain structurally intact
  - Seismic Category 1B for active components that are required to remain structurally intact and functional
- **Seismic Category 2** – SSCs that are not required to remain functional during or after a seismic event, but whose failure during a seismic event could adversely affect the ability of any Seismic Category 1A or 1B SSCs to accomplish its Safety Category 1 function.

- **Seismic Category RW -** SSCs for management and storage of radiological material that meet the criterial for RW-IIa (High Hazard) in U.S. Nuclear Regulatory Commission (USNRC) Regulatory Guide (RG) 1.143 “Design Guidance for Radioactive Waste Management Systems, Structures and Components Installed in Light-Water-Cooled Nuclear Power Plants”, (Reference 3-46) are classified as Seismic Category RW. RG 1.143 permits the use of the ASCE/SEI 43, “Seismic Design Criteria for Structures, Systems and Components in Nuclear Facilities,” (Reference 3-47) graded approach for the seismic classification of SSCs with justification. These SSCs are therefore designed to remain essentially elastic without any significant permanent deformation up to half of the Design Basis Earthquake (DBE). The use of the ½ DBE is justified as it bounds the ground motion spectra for seismic categories identified in ASCE/SEI 43 (Reference 3-47) for SSCs used for handling and storage of highly radioactive materials.
- **Seismic Category NS** - All other SSC are categorised as Non-Seismic (NS) and are designed based on applicable non-nuclear requirements.

See NEDC-34186P, “BWRX-300 UK GDA Ch. 15.8: Safety Analysis: External Hazards,” (Reference 3-23) for further discussion on the application of the one-half site-specific DBE approach for BWRX-300 Seismic Category RW SSCs in the UK.

The BWRX-300 Containment and the Reactor Building (RB) are the only structures that house, support, or protect BWRX-300 SC1 SSCs. These two structures are therefore categorised as BWRX-300 Seismic Category 1A structures in the BWRX-300 design.

Seismic Interaction

SSCs that are not BWRX-300 Seismic Category 1A or 1B, but whose failure during a seismic event could adversely affect the ability of any Seismic Category 1A or 1B SSCs to accomplish its safety function, are evaluated for seismic interaction to demonstrate that:

- These SSCs will not collapse or collide with the BWRX-300 Seismic Category 1A or 1B SSCs and will maintain their stability during a DBE or other relevant extreme external hazard event
- Impact loads that result from collapse or collision on the BWRX-300 Seismic Category 1A or 1B SSCs are either negligible or smaller than those considered in the design

Interaction evaluations are performed of the Power Block structures and foundations adjacent to the RB to ensure:

- These structures and foundations do not collapse to compromise the safety functions of those SSCs that are required to remain functional following a DBE or design extreme wind level event for the first 72 hours.
- The Control Building (CB) structure, which includes the Main Control Room (MCR) does not collapse and result in incapacitating injury to the MCR occupants or prevent their egress to the RB.

3.2.4 Quality Group

BWRX-300 pressure-retaining components are designed to ensure they are protected against overpressure conditions, and are classified, designed, fabricated, erected, inspected, and tested in accordance with established standards. The selection of codes and standards is commensurate with the SC and is adequate to provide confidence that plant failures are minimized.

BWRX-300 design utilises a Quality Group designation per the guidance in USNRC RG-1.26, “Quality Group Classifications and Standards for Water-, Steam-, and Radioactive-Waste-Containing Components of Nuclear Power Plants,” (Reference 3-48) as a

method for establishing the appropriate codes and standards based on the importance of the pressure-retaining function of the component. Items are classified as Quality Group A, B, C or The guidance and classification method are used with some clarification based on the unique design of the BWRX-300.

One exception is taken to the guidance in RG 1.26 with respect to RPV Isolation Valves, as initially discussed in NEDC-33911P-A, “BWRX-300 Containment Performance”. RPV isolation valves that function as the inboard Containment Isolation Valves (CIVs) are designed in accordance with the rules and requirements of American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code (BPVC), Section III, Division 1, Subsection NB, Class 1 Components.

Table 3-3 tabulates the design and fabrication requirements for each Quality Group. For mechanical equipment that does not fall within the scope of USNRC RG 1.26 (Reference 3-48), appropriate industrial codes and standards are applied.

3.3. Protection Against External Hazards

The BWRX-300 design considers natural and human-induced external hazards that may be linked with significant radiological risk. This section discusses external hazards and the BWRX-300 approach to prevent and mitigate their effects on SC1 SSCs. SC2/SC3 SSCs that are credited in the fault evaluation with mitigating fault sequences initiated by external hazards, and SSCs whose failure can affect the structural integrity or SC functions of adjacent SC1 SSCs are also protected against external hazards.

The determination of the external hazards considered in the BWRX-300 design relies on the collection of the geotechnical, seismological, hydrological, hydrogeological, and meteorological reference data, and human-induced external events presented in NEDC-34196P, “BWRX-300 UK GDA Ch. 2: Site Characteristics,” (Reference 3-55). For external hazards, the main protection is provided by the civil structures. The design against external hazards is such that a design basis external hazard does not lead to a DBA or a BDBA. Significant safety margins are included in the evaluation of the design basis external hazards and the associated design aspects to ensure a conservative design. Assurance that the overall reactor plant is resilient to external hazards is provided by the demonstration that SSCs do not fail when subject to these hazards and generated loadings. Demonstration of the adequacy of protection measures is provided in the applicable PSR chapters covering the design of SSCs.

Malevolent acts considered in the robustness design are discussed in Section 3.3.3 of Attachment 1 in NEDC-34165P (Reference 3-1), (Other External Hazards – Robustness Against Malevolent Acts).

Protection and mitigation methods considered in the design are in line with the design safety objectives and D-in-D concept discussed in PSR Ch. 2, Sections 2.1 and 2.6, respectively. They include the use of physical separation, barriers/shielding, qualification of equipment and instrumentation for the hazards environment and monitoring programs to preclude unacceptable radiation releases following accidents due to external hazards.

When applicable, loads generated by external hazards are considered in the BWRX-300 design. Combination of loads from randomly occurring individual external hazards is considered in the design to ensure structures are adequately protected against external hazards.

A principal safety objective of the BWRX-300 Safety Strategy is the demonstration that the overall reactor plant design is resilient to hazards through D-in-D. This means that the design provisions optimize protection to provide the highest level of safety that can reasonably be achieved such that relevant dose targets on-site and off-site are met and the resilience of the reactor plant to external hazards reduces risk. The process of demonstrating that the reactor plant is resilient starts with the systematic identification of PIEs with a potential to challenge a fundamental safety function, and to organize them into the fault list developed as per NEDC-34178P (Reference 3-15). Combinations of randomly occurring individual events are considered in these evaluations. Deterministic and probabilistic safety analyses are then performed as discussed in NEDC-34183P (Reference 3-20) and PSR Ch. 15.6 (Reference 3-21), to confirm the design adequacy and its resilience to these hazards.

See Section 3.3 of NEDC-34165P Attachment 1 (Reference 3-1) for further detail on protection against external hazards.

3.4. Protection Against Internal Hazards

This section discusses design basis internal hazards that could compromise the safety functions of SC1 SSCs and preventive, and mitigation measures implemented in the design to eliminate their adverse effects. SC2/SC3 SSCs credited in the fault evaluation with mitigating fault sequences initiated by internal hazards are also protected against internal hazards. For BDBA internal hazards, refer to NEDC-34178P (Reference 3-15).

The list of internal hazards considered in the BWRX-300 design is generated from the industry guidelines and the specifics of the BWRX-300 technology. Screening methodology of internal hazards for safety analysis purposes and ultimately confirmation of adequacy of protection measures is identical to that of the external hazards presented in Attachment 1, Section 3.3 of NEDC-34165P (Reference 3-1).

Protection and mitigation methods considered in the design are in line with the design safety objectives and D-in-D concept discussed in Sections 3.1.1 and 3.1.7, respectively. They include the use of separation, barriers/shielding and monitoring programs as described in Section 3.1.2 to preclude unacceptable radiation releases following accidents due to internal hazards.

Combination of loads from randomly occurring individual internal hazards is also considered in the design to ensure structure are adequately protected against internal hazards.

See Section 3.4 of NEDC-34165P, Attachment 1 (Reference 3-1), for further detail on protection against internal hazards.

3.5. Design of Civil Structures

Section 3.5 of NEDC-34165P, Attachment 1 (Reference 3-1) presents the general design principles, general design basis requirements and general criteria used in the design of the BWRX-300 civil structures, including their foundations.

3.6. Mechanical Systems and Components

Section 3.6 of NEDC-34165P Attachment 1 (Reference 3-1) provides the general design aspects used for SC and Non-Safety Class (SCN) mechanical systems and components. It includes special considerations for mechanical components, dynamic testing, and analysis of SSCs, required codes for ASME BPVC Section III, Division 1, Class 1, 2, and 3 components, and Subsection NF for component supports, and Subsection NG for core support structures. In addition, general design aspects for Control Rod Drive (CRD) system, and reactor vessel internals are presented. Further, this section discusses the functional design, qualification, and In-Service Testing (IST) program requirements for pumps, valves, and dynamic restraints.

The general design principles, criteria, and classification used for design of mechanical systems and components have been discussed earlier in PSR Ch. 3. Among these principles are design for robustness, reliability, and fail-safe operation. Additionally, the systems and components are required to be redundant, diverse, independent, separate, and of supply quality that is commensurate with the safety classification and seismic category. The design and qualification of mechanical components is performed using a graded approach with the highest level of rigor applied to SC1 components.

Section 3.6 in NEDC-34165P Attachment 1, (Reference 3-1) also develops the seismic input criteria and building spectra used as input for seismic qualification of Seismic Category I active mechanical components and system functionality. Additionally, Seismic Category I passive mechanical component supports, and equipment supports use the seismic spectra for qualification.

Equipment qualification requirements are provided in Section 3.9 of PSR Ch. 3 for seismic and dynamic qualification of mechanical and electrical equipment, and provides the equipment qualification requirements including environmental, functional qualification, and Electromagnetic Compatibility (EMC), which are used as input to safety classified mechanical systems and components.

3.7. General Design Aspects for Instrumentation and Control Systems and Components

The BWRX-300 Distributed Control and Information System (DCIS) is an integrated control and monitoring system for the power plant. The DCIS is arranged in three safety classified DCIS segments that have appropriate levels of hardware and software quality corresponding to the system functions they control and their allocation to the DLs. The DCIS provides control, monitoring, alarming and recording functions. Although normally integrated, the various components of the DCIS are designed to operate independently.

See Section 3.8 in Attachment 1 of NEDC-34165P (Reference 3-1), Section 3.8 for further discussion on the general design aspects, and NEDC-34169P (Reference 3-6) for further detail on the I&C systems and components.

3.8. General Design Aspects for Electrical Systems and Components

The electrical power system design is a 50 Hz Alternating Current (AC) power system, with 6.9 kV for the Medium Voltage (MV) level and 690 VAC (Volts Alternating Current), and 400/230 VAC for the Low Voltage (LV) level.

The BWRX-300 design minimises the reliance on electrical power to support safety category functions. The passive design of the plant is not dependent upon AC power sources including diesel generators, to mitigate a DBA. SC1 power is supplied from battery-backed Direct Current (DC) power, which has a coping period of 72 hours for all DBAs.

See Section 3.8 in Attachment 1 of NEDC-34165P (Reference 3-1), for further discussion on the general design aspects, and NEDC-34170P (Reference 3-7) for further detail on the electrical systems and components.

3.9. Equipment Qualification

3.9.1 Introduction

Purpose

Equipment qualification is the process carried out (including the generation and maintenance of evidence) to ensure SSCs can perform their intended design functions and remain fit for purpose in the conditions under which they are expected to perform.

The conditions impacting equipment qualification include seismic/dynamic, environmental, functional/aging stressors, and electromagnetic interference.

Scope

Equipment qualification requirements are applied to BWRX-300 equipment based on the assigned safety classification and seismic categorisation of SSCs (as described in Section 3.2.3), and to certain post-accident monitoring equipment.

Equipment qualification considers all normal operating conditions in which the SSCs are expected to operate including conditions arising from maintenance and testing, and also, the conditions arising from AOOs, DBAs, and internal and external hazards.

DEC survivability assessments are outside the scope of a qualification program. However, IEC/IEEE 60780-323, “Nuclear facilities – Equipment important to safety – Qualification,” (Reference 3-56) considers qualifying equipment for DEC and the guidance IEC/IEEE 60980-344, “Nuclear facilities – Equipment important to safety – Seismic qualification,” (Reference 3-57) can be used to demonstrate with reasonable confidence, that SSCs will survive and perform their intended fundamental safety function(s) under the expected conditions for the timespan required.

Aging Considerations

Significant aging mechanisms are considered in establishing EQ for the specified service conditions and in defining the qualified life of equipment and components. An aging mechanism is significant if subsequent to manufacture, while in storage, and/or in the normal and abnormal service environment, it results in degradation of the equipment that progressively and appreciably renders the equipment vulnerable to failure to perform its SC function under harsh environmental DBA conditions. These typically include thermal, radiation, and operation induced degradation. Age conditioning is used during qualification to simulate these effects. Age conditioning considers sequential, simultaneous, and synergistic effects to achieve the worst state of degradation.

For equipment that cannot meet the required cycles for the 60-year life, a shorter qualified life is established, and the effects of physical aging and obsolescence are reflected in the maintenance, surveillance, and replacement program.

3.9.2 Seismic and Dynamic Qualification of Mechanical and Electrical Equipment

The BWRX-300 Seismic Category 1A or 1B (hereafter referred as Seismic Category I) mechanical and electrical equipment (including I&C components) are designed to withstand the effects of earthquakes (i.e., Seismic Category I requirements), and other accident-related dynamic loadings.

Mechanical equipment consists of items of a facility including pumps, valves, valve operators, vessels, and piping whose function is required to ensure safe operation or safe shutdown. Electrical equipment consists of all electrical power and I&C equipment, which includes all analog (non-digital) and digital I&C components. Computer-based I&C equipment is a subset of digital I&C components. Examples of electrical equipment are battery and battery racks, instrument and instrument racks, control consoles, electrical cabinets, electrical panels, valve

operator motors, solenoid valves, pressure switches, relays, level transmitters, electrical penetrations, and pump and fan motors.

Structures, Systems, and Components (SSCs) that are credited to remain functional during or after a seismic event are Seismic Category I. SSCs whose failure during a seismic event could adversely affect the ability of Seismic Category I SSCs to accomplish their fundamental safety functions are considered for the qualification.

Section 3.9.2 addresses dynamic testing of components of the RCPB to ensure it can withstand the applicable design-basis seismic and dynamic loads in combination with other environmental and natural phenomena loads without leakage, rapidly propagating failure, or gross rupture.

The methods of test and analysis employed to ensure the operability of mechanical and electrical equipment are based on joint standard International Electrotechnical Commission (IEC)/Institute of Electrical and Electronics Engineers (IEEE) 60980-344 (Reference 3-57). Regulatory Guide (RG) 1.100 endorses IEEE-344-2013. The BWRX-300 design utilizes IEC/IEEE 60980-344. The additional guidance provided in RG 1.100 is used to identify individual components of the RCPB demonstrating through testing and analysis, or a combination of both, that a given component will not leak as a result of any combination of loadings for which it is qualified. This ensures that components are tested to the highest quality standards practical.

Seismic design and design of Seismic Category I SSCs are addressed in NEDC-34165P Attachment 1 (Reference 3-1).

Seismic and Dynamic Qualification Criteria

A determination of the criteria for seismic and dynamic qualification is dependent on the type of equipment to qualify either mechanical, electrical, and/or I&C and the required seismic and dynamic inputs necessary to demonstrate structural and/or functional integrity. The criteria is provided in the following sections.

Qualification Standards

The guidance provided in the ASME BPVC Section III Division 1 “Rules for Construction of Nuclear Facility Components” is followed in the design of SC1 mechanical equipment to achieve the structural integrity of pressure boundary components. SC1 valves consider the qualification guidance provided in ASME QME-1, “Qualification of Active Mechanical Equipment Used in Nuclear Facilities,” (Reference 3-58), for their qualification program.

Seismic and dynamic qualification of mechanical and electrical equipment and associated supports are considered for testing, analysis, or a combination of testing and analysis in accordance with IEC/IEEE 60980-344 (Reference 3-57) in accordance with RG 1.100.

Qualification by Actual Seismic Experience

IEC/IEEE 60980-344 (Reference 3-57) provides experience based seismic qualification methodology and is utilized as appropriate. In addition, ASME QME-1 (Reference 3-58) seismic experience may be utilised as appropriate. The information includes the credibility and completeness of compilation of the earthquake experience database for the seismic qualification of electrical equipment. The inclusion and exclusion rules for electrical equipment in the experience database, the justification used to demonstrate the similarity among the member items in a reference equipment class, the justification used to demonstrate the similarity between electrical equipment in the experience database and equipment in the Nuclear Power Plant (NPP) for seismic qualification purposes, and the justification used to demonstrate the functionality of equipment and the member items in a reference equipment class during and after a seismic event.

Qualification by Similarity

Qualification by similarity for Seismic Category I and 2 equipment is based on operating experience of similar equipment or to qualify multiple similar pieces of equipment by testing and/or analysing only one of the pieces of equipment. When extrapolation of data is made from similar equipment, a description of the differences between the equipment items involved is required. Justification that the differences do not degrade the environmental and/or seismic adequacy below acceptable limits and any additional supporting data is included.

Test results can be extrapolated for dynamic loading conditions in excess of, or different from, previous tests on a piece of equipment if the test results are in sufficient detail to allow an adequate dynamic model of the equipment to be generated. The model provides the capability of predicting failure under the increased or different dynamic load excitation. IEC/IEEE 60980-344 (Reference 3-57) defines the analytical method utilised in similarity qualification.

Functional Qualification of Active Mechanical Equipment

The seismic qualification of active mechanical equipment is performed considering the methods and requirements specified in ASME QME-1 (Reference 3-58).

Qualification Program

The equipment qualification program follows the requirements provided in IEC/IEEE 60780-323 (Reference 3-56), and is used to determine the overall equipment qualification test plan, including EQ provided in Section 3.9.3. The program meets the qualification criteria contained in IEC/IEEE 60980-344 (Reference 3-57) that includes seismic and dynamic mechanical and electrical equipment qualification.

Seismic Qualification Report

The seismic qualification report follows the requirements that are defined in IEC/IEEE 60980-344 (Reference 3-57) and is specific to the Seismic Category I electrical and mechanical equipment and associated supports to be qualified.

Methods and Procedures for Qualifying Mechanical and Electrical Equipment

Seismic Input Motion

Dynamic load conditions are simulated by testing using independent, random multi-frequency input or single frequency input motion (within equipment capability) over the frequency range of interest.

Acceptable justification for use of single frequency input includes, but is not limited to:

- The characteristics of the required input motion are dominated by one frequency
- The anticipated response of the equipment is adequately represented by one mode
- The input has sufficient intensity and duration to excite all modes to the required magnitude so that the testing response spectra envelop the corresponding response spectra of the individual modes
- The time phasing of the inputs in the vertical or horizontal directions is such that a purely rectilinear resultant input is avoided

The actual input motion used during testing, for both multi and single frequency, envelops the applicable input motion (floor, wall, response, etc.) at the location(s) of the equipment under test.

When the equipment is qualified by dynamic test, the in-Structure Response Spectra (ISRS) or time histories are used in determining Required Response Spectra (RRS) of input motion used for the test.

When both test and analysis are defined as acceptable methods, the deciding factors considered (as applicable) for choosing between tests or analysis includes:

- Magnitude of accelerations and frequency content of seismic and Reactor Building Vibration (RBV) dynamic loadings
- Environmental conditions associated with the dynamic loadings
- Nature of the function(s) required for a seismic event
- Size and complexity of the equipment
- Dynamic characteristics of expected failure modes (structural or functional)
- Partial test data upon which to base the analysis

Tests or analyses of assemblies are preferable to tests or analyses on separate components (e.g., a motor and a pump, including the coupling and other appurtenances, should be tested, or analysed as an assembly). The replacement parts may be tested separately, if applicable.

Equipment that has been previously qualified by means of tests and analyses equivalent to those required for the current qualification program are used if proper documentation of such tests and analyses is available.

Qualification by Testing

Seismic qualification of mechanical and electrical equipment including I&C by testing is performed in accordance with the requirements of IEC/IEEE 60980-344 (Reference 3-57).

Interface Requirements

Intervening structures or components (such as interconnecting cables, bus ducts, conduits) that serve as interfaces between the equipment to be qualified and that are supplied by others, are not qualified as part of the seismic equipment qualification program. When applicable, accelerations and frequency content at locations of interfaces with interconnecting cables, bus ducts, and conduits are determined and documented. This information is specified in the form of interface criteria.

Test Methods

The test methods presented in IEC/IEEE 60980-344 (Reference 3-57) provide acceptable types of testing dependent on the type of motion selected based on the expected vibration environment and technical requirements of the specific application.

The preferred method for seismic testing is to use triaxial, multi-frequency testing. However, if justified, biaxial and single-axis testing is acceptable. If biaxial testing is justified to be used, then each test is performed in two steps, where the first step is to apply the input motion to both the vertical and horizontal axis simultaneously. For the second step, the test specimen is rotated 90 degrees in the horizontal plane, and a second test is performed with the input motion applied to the vertical and horizontal axis. Therefore, biaxial testing at a minimum requires twice the number of runs as triaxial testing. The preferred method for biaxial testing is independent, random tests.

For biaxial testing, when independent, random tests are not available, four tests are performed:

- With the inputs in phase
- With one input 180 degrees out of phase

- With the equipment rotated 90 degrees horizontally and the inputs in phase
- With the same orientation as in the step (3), but with one input 180 degrees out of phase

Selection of Test Specimen

Representative samples of equipment and supports are selected for use as test specimens. Variations in the configuration of the equipment are analysed with supporting test data. Test specimen assemblies that represent multiple configurations are configured to represent the "worst case" configuration. For example, these variations may include mass distributions that differ from one cabinet to another. Therefore, it is analysed and justified which mass distribution(s) results in the maximum stresses, such as response accelerations or frequency content, and this worst case configuration(s) is used as the test specimen(s).

Mounting of Test Specimen

The test specimen is mounted to the test table so that the installed configuration, including interfaces, is adequately simulated and differences between the configuration are evaluated and resolved. If the test specimen is intended to be mounted to a panel or enclosure, the panel, enclosure, or a test fixture representative of the mounting conditions is included in the testing, unless justified. If the test specimen cannot be mounted directly to the table due to mounting constraints, an interposing test fixture is designed and used as the mounting interface. However, the equipment-to-fixture mounting condition is to simulate its installed configuration and cause no dynamic coupling to the equipment. If the equipment being analysed has no required orientation, the worst possible orientation is considered. The test specimen is considered to be in its operational configuration (i.e., filled with the appropriate fluid and/or solid). The investigation ensures that the point of maximum stress is considered. The test specimen mounting, and configuration includes hardware interface requirements. For interfaces that cannot be simulated on the test table, the accelerations and any resonances at such interface locations are recorded during the equipment test and documented in the test report.

Aging and Vibration Conditioning

The testing simulates the effects of aging. Equipment is reviewed in terms of design, function, materials, and environment for its specified application to identify potentially significant aging mechanisms.

If equipment is subjected to vibrational loads throughout its lifetime in its in-service mounted condition, then vibration aging to its end-of-life condition is performed prior to seismic qualification when required by the applicable qualification standard(s).

Qualification by Analysis

Qualification by analysis without testing may be acceptable on equipment that is only required to maintain its structural integrity to perform its safety function as described in IEC/IEEE 60980-344 (Reference 3-57).

Dynamic analysis or an equivalent static analysis is employed to qualify the equipment when analysis is chosen as the method for qualification. The decision on using dynamic versus static analysis is typically defined based on whether the equipment is rigid or flexible.

If the fundamental frequency of the equipment is above the input excitation frequency (cutoff frequency of RRS), the equipment is considered rigid. The search for the natural frequency is done analytically, if the equipment shape is defined mathematically, or by prototype testing.

If the equipment is determined to be a rigid body (i.e., shown to have no resonance frequency within the expected frequency range), the static analysis method is able to be applied in place of dynamic analysis.

If the equipment is determined to be flexible (i.e., with the fundamental frequency of the equipment within frequency range of the input spectra) and not simple enough for equivalent static analysis, a dynamic analysis method is applied, unless justified otherwise.

If it is determined either dynamic or static analysis can be used, in general, the choice of the analysis is based on the expected design margin because the static coefficient method (the easiest to perform) is far more conservative than the dynamic analysis method.

For static analysis, the dynamic forces on each component can be obtained by concentrating the mass at the center of gravity and multiplying the mass by the appropriate floor acceleration. The dynamic stresses are then added to the operating stresses and a determination is made of the adequacy of the strength of the equipment.

A static coefficient analysis may also be used for certain equipment in lieu of the dynamic analysis. No determination of natural frequencies is made in this case. The seismic loads are determined statically by multiplying the actual distributed weight of the equipment by a static coefficient equal to 1.5 times the peak value of the RRS at the equipment mounting location, at a conservative and justifiable value of damping.

Both types of analyses are to verify integrity of the equipment is maintained under low level earthquake loads, including appropriate RBV dynamic loads in combination with normal operating loads, and Safe Shutdown Earthquake (SSE) loads, including appropriate RBV dynamic loads, unless otherwise justified.

NEDC-34165P Attachment 1 (Reference 3-1) defines acceptable load combinations and methods for combining dynamic responses for mechanical equipment. The same criteria are acceptable for electrical equipment.

Qualification by Combined Testing and Analysis

Qualification by combined testing and analysis is used as a method for qualification for complex or large equipment where it is not practical to test the entire assembly or it is too large to be tested at once, unless another method of qualification is justified.

One method of combined qualification is to use a representative prototype portion or scaled-down prototype of the assembly that is subjected to type testing. The data from the type testing is then used to develop and validate an analytical model of the prototype. The prototype analytical model is then extrapolated to represent the larger assembly and the results used to justify qualification of the equipment based on prototype testing.

A second method of combined qualification is to mount the full assembly to a rigid floor to simulate service mounting, and then a portable shaker test (or an impact or pull test if justified) is performed to excite the natural or resonance frequencies of the specimen. The amplification of resonance motion is used to determine the appropriate modal frequency and damping for a dynamic analysis of the equipment.

For equipment with multiple site configurations, the combined qualification method can be applied to reduce the number of configurations to be tested. In this case, an evaluation must be performed to determine the enveloping “worst-case” configuration(s), which is then tested. Analysis is then used to justify the various configurations based on the “worst-case” configuration(s).

The combination method is used for qualification of larger electrical equipment support assemblies containing SC1 equipment where it is not practical to test the entire assembly or it is too large to be tested at once, unless another method of qualification is justified. For this case, a test is run to determine if there are natural frequencies in the support equipment within

the critical frequency range (any frequency below the cutoff frequency on the response spectrum). If the support is determined to be free of natural frequencies in the critical frequency range, then it is assumed to be rigid, and a static analysis is performed and calculations of transmissibility and responses to varying input accelerations are determined to see if SC1 equipment mounted in the assembly would operate without malfunctioning.

For digital I&C equipment qualification in a mild environment, analysis can be used in addition to testing if there is testing of an identical or similar item, or there is operating experience of equipment under identical or similar conditions with a supporting analysis to show that the equipment to be qualified is acceptable. Also, I&C equipment qualification can be performed using an analysis in combination with partial type test data that supports the analytical assumptions and conclusions.

Methods and Procedures of Analysis or Testing of Supports for Mechanical, Electrical Equipment and Instrumentation

Methods and procedures of analysis or testing of supports for mechanical and electrical equipment and instrumentation are in accordance with IEC/IEEE 60980-344 (Reference 3-57) and ASME QME-1 (Reference 3-58).

Supports for Battery Racks, Instrument Racks, Control Consoles, Cabinets, and Panels

SC1 control boards, panels, and racks should consider the qualification guidance provided in IEEE 420, “IEEE Standard for Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations,” (Reference 3-59), for their qualification program.

Cable Trays and Conduit Supports

SC1 cables consider the qualification guidance provided in IEEE 383, “IEEE Standard for Qualifying Electric Cables and Splices for Nuclear Facilities,” (Reference 3-60), and IEEE 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” (Reference 3-61), and test requirements in IEEE 1202, “IEEE Standard for Flame-Propagation Testing of Wire and Cable,” (Reference 3-62) are used for the qualification program.

Supports provided by the equipment supplier to be used for the equipment is to be qualified in accordance with this section by the equipment supplier.

Seismic Category I supports (hangers) that support trays or conduit that carry safety circuits are designed and analysed to demonstrate qualification in accordance with IEEE 628, “IEEE Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations,” (Reference 3-63).

SC1 connection assemblies consider the qualification guidance provided in IEEE 572, “IEEE Standard for Qualification of Class 1E Connection Assemblies for Nuclear Power Generating Stations and Other Nuclear Facilities,” (Reference 3-64) for the qualification program as endorsed by RG 1.156, “Qualification of Connection Assemblies for Production and Utilization Facilities,” (Reference 3-87).

Line Mounted Equipment

IEC/IEEE 60980-344 (Reference 3-57) identifies special consideration is required for line-mounted (piping and duct system) equipment regarding seismic qualification as the most critical seismic loading condition can occur as a result of the piping or duct system.

Guidance and further clarification for special considerations for line-mounted equipment are provided in IEC/IEEE 60980-344 (Reference 3-57) as well as IEEE 382, “IEEE Standard for Qualification of Safety-Related Actuators for Nuclear Power Generating Stations and Other Nuclear Facilities,” (Reference 3-65). Line-mounted equipment may also include active

mechanical equipment subjected to ASME QME-1 (Reference 3-58), including the QR-A Non-mandatory Appendix.

3.9.3 Environmental Qualification of Mechanical and Electrical Equipment

EQ includes the generation and maintenance of evidence to ensure SSCs can perform their intended design functions and remain fit for purpose in the conditions under which they are expected to perform. Section 3.9.2 provides the methodology and requirements used for the seismic and dynamic qualification of Seismic Category I Mechanical and Electrical equipment.

Mild Environment

An environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including AOOs, and does not give rise to significant aging mechanisms.

Harsh Environment

An environment that significantly changes from normal including design basis events and post-accident conditions as a result of a DBA.

AOO Environment

AOO environmental conditions are the service conditions as a result of an operational deviation expected to occur during the operating plant lifetime that do not lead to accident conditions.

The methodology and requirements apply to the EQ of SC1 mechanical and electrical equipment, including I&C, located in harsh and mild environments. IEC/IEEE 60780-323 (Reference 3-56), as endorsed by USNRC RG 1.89, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” (Reference 3-68), defines the methodology and criteria used to qualify SC1 equipment for harsh and mild environments for the BWRX-300.

The environmental conditions in which the instrumentation and equipment of the SC1 systems operate are considered in establishing the component specifications. Instrumentation specifications are based on the worst expected ambient environmental conditions in which the instruments operate.

Qualification of mechanical equipment that performs a safety function is in accordance with ASME QME-1 (Reference 3-58).

Equipment Identification and Environmental Conditions

Equipment Identification

The equipment qualification program generates and maintains a list of SC1 equipment located in harsh and mild environments. The qualification plan includes the following parameters, at minimum and as applicable: the test and/or analysis sequence, environmental and/or seismic/dynamic or EMC requirements, test item functions, identification of industry codes and standards applicable to equipment, identification of the test equipment including description and calibration plan, and test item part numbers, quantity, mounting, and connection details.

Environmental Conditions

General Requirements

Environmental Design Bases

The environmental conditions consider normal, AOO, accident, and post-accident conditions, as applicable. Equipment located below the maximum flood level considers the effects of submergence and is qualified for flooding if it is required to function in this condition. Post-accident monitoring equipment considers the criteria for accident monitoring instrumentation

and EQ guidance provided in IEEE 497, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,” (Reference 3-66), as endorsed by RG 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” (Reference 3-67).

The harsh environment qualification program verifies that the equipment is designed to be compatible and perform its safety functions during normal conditions, postulated environmental conditions, DBA, and post-accident conditions.

Equipment located within harsh environment conditions is exposed to environmental conditions including temperature, pressure, relative humidity, radiation, and chemical sprays.

Equipment determined to have a significant aging mechanism and located in a harsh environment account for the aging mechanism in the qualification program.

Aging mechanisms to be analysed for equipment located in a harsh environment include time-temperature degradation (thermal), cycle aging (wear), and normal radiation exposure.

Analysis is performed to identify the environmental design bases for AOOs, normal, accident, and post-accident environments as applicable.

Equipment is qualified to the worst-case environmental conditions for the areas in which they are located for the duration that they are required to perform their SC1 function.

The Safety Category 1 functions are either functional performance requirements or fail-safe requirements. A fail-safe SC1 function consists of not failing in a manner detrimental to plant safety, accident mitigation, or prevention of a SC1 function. The basis for the Safety Category 1 function is included in the qualification documentation.

Although EQ by testing or analysis is not required for SC2 and SC3 components, these components are designed for their expected duty cycle and environmental conditions over the design life of the plant with due consideration for maintenance and aging management. Additionally, SC2 and SC3 components that perform a SC1 function are qualified to the specified environmental conditions by testing or analysis.

The environments are considered for electrical and mechanical equipment in the EQ program such as temperature, pressure, humidity, chemical effects, radiation, and flooding effects. The EQ program uses the recommended environmental margins per IEC/IEEE 60780-323 (Reference 3-56), Table 1.

Aging requirements apply to SC1 equipment. For equipment located in harsh and mild environments, the effect of aging is be performed prior to DBA testing when a significant aging mechanism exists. Equipment is reviewed in terms of design, function, materials, and environment for its specified application to identify potentially significant aging mechanisms.

Equipment that could be exposed to radiation is environmentally qualified to a radiation dose that simulates the calculated radiation environment (normal and accident) that the equipment can withstand prior to completion of its required safety functions.

Radiation qualification considers that equipment damage is a function of total integrated dose and can be influenced by dose rate, energy spectrum, and particle type. The radiation qualification includes doses from all potential radiation sources at the equipment location. For equipment that is required to be functional post-accident, then the radiation dose is increased beyond the dose required for qualified life to envelop post-accident conditions as well, unless it is determined to cover post-accident conditions separately.

A mild radiation environment for electronic equipment is defined as a total integrated dose less than 10 gray (Gy) (1.0E03 rad), and a mild radiation environment for other equipment is less than 100 Gy (1.0E04 rad) as defined in RG 1.89 (Reference 3-68).

Electronic and electrical equipment are tested with the equipment energized and performing its safety function if the required total integrated dose exceeds the mild environment level. This ensures equipment is qualified for the worst-case radiation with DBA margin per the requirements of IEC/IEEE 60780-323 (Reference 3-56).

Electromagnetic Interference / Radio Frequency Interference and Voltage Surges

EMC requirements apply to all levels of SC equipment, SC1, SC2, SC3, and SCN and provides qualification methods and implementation guidance. EMC qualifications for BWRX-300 design follow the requirements defined in (1) EPRI TR-102323, “Guidelines for Electromagnetic Compatibility Testing of Power Plant Equipment,” (Reference 3-69), or (2) Military Standards MILSTD-461G, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” (Reference 3-70), or (3) IEC-62003, “Nuclear Power Plants – Instrumentation, Control, and Electrical Power Systems – Requirements for Electromagnetic Compatibility Testing,” (Reference 3-71). The qualification for Electromagnetic Interference/Radio Frequency Interference (EMI/RFI) and voltage surges for EQ equipment in harsh and mild environments is by test, consistent with USNRC RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” (Reference 3-72) “Guidelines for Evaluating Electromagnetic and Radio Frequency Interference in Safety Related Instrumentation and Control Systems”. EMC Qualification and Acceptance Testing includes tests for susceptibility and emissions. Susceptibility and emissions requirements are applied to all SC and SCN microprocessor-based I&C and electrical equipment.

Qualification Tests and Analyses

Qualification

Type testing is the preferred method for demonstrating that equipment is Environmentally Qualified. A type test subjects a representative sample of equipment, including interfaces, to a series of tests, and includes simulating the effects of significant aging mechanisms during normal operation. The sample is subsequently subjected to conditions that simulate DBA harsh conditions and thereby establishes the tested configuration for installed equipment service, including mounting, orientation, interfaces, conduit sealing, and expected environments. A type test demonstrates that the equipment performs the intended Safety Category function(s) for the required operating time before, during, and/or following the DBA, as appropriate.

Tests are performed in accordance with applicable industry standards, such as IEC/IEEE 60780323 (Reference 3-56).

Qualification by Analysis

In general, analysis is used to supplement test data and the analytical techniques and modelling assumptions are, when possible, based on a correlation of the analytical approach with testing or operating experience performed on similar equipment or structures.

Seismic and dynamic qualification by analysis is described in Section 3.9.2.

For qualification by analysis, a logical assessment, or a valid mathematical model of the equipment to be qualified is required, and the basis for the analysis includes physical laws of nature, results of test data, operating experience, and condition indicators, as applicable.

Analysis of data and tests for material properties, equipment rating, and environmental tolerance are acceptable methods to be used to demonstrate qualification.

Analysis alone is not used to demonstrate the initial qualification for electrical equipment in a harsh environment.

Qualification by Operating Experience

Qualification by use of operating experience requires documented data to be available confirming to the following conditions are met:

- The product providing the operating experience is identical or justifiably similar to the equipment to be qualified
- The product providing the operating experience has operated under service conditions which equal or exceed, in severity the service conditions and performance requirements for which the product is to be qualified are bounded by the product providing the operating experience
- The installed product in general, is removed from service and subjected to partial type testing to include the DBA environments for which the product is to be qualified

Combined Qualification

Combination of test and analysis is used when it is deemed practical to use both methods to complete the qualification. The combined qualification method can be used for qualification for larger electrical equipment where it is not practical to test the entire assembly, or it is too large to be tested at once, unless another method of qualification is justified.

For digital I&C equipment qualification in a mild environment, analysis can be used in addition to testing if there is testing of an identical item of equipment under identical conditions or under similar conditions or operating experience with a supporting analysis to show that the equipment to be qualified is acceptable. Also, I&C equipment qualification can be performed using an analysis in combination with partial type test data that supports the analytical assumptions and conclusions.

Specific Equipment Requirements

Mechanical Equipment

SC1 mechanical equipment, which has the sole Safety Category 1 function of maintaining pressure integrity, and which is designed, fabricated, and qualified consistent with ASME BPVC, Section III, “Rules for Construction of Nuclear Facility Components,” (Reference 3-73), is considered qualified.

For mechanical equipment where the loading under normal service is more severe than loading under DBA, then the loading under normal service is considered in addition to the loading under DBA by test and/or analysis.

For mechanical equipment, the loading and capability under DBA conditions is analysed in the qualification process to establish the suitability of materials, parts, and equipment needed for safety functions, and to verify that the design of such materials, parts, and equipment is adequate.

The qualification of mechanical equipment includes, as applicable, materials that are sensitive to environmental effects (e.g., seals, gaskets, lubricants, fluids for hydraulic systems, and diaphragms), required operating time, non-metallic subcomponents of such equipment, the environmental conditions and process parameters for which this equipment is qualified, non-metallic material capabilities, and the evaluation of environmental effects.

In addition, the qualification guidance provided in ASME QME-1 (Reference 3-58) is considered for qualification of SC1 valves and SC1 mechanical pipe supports. The qualification of non-metallic parts considers the qualification guidance provided in the Nonmandatory Appendix QR-B of ASME QME-1 (Reference 3-58).

Electrical Equipment

Additional qualification guidance is considered for specific electrical equipment, if applicable, as follows:

- RG 1.158 “Qualification of Safety-Related Vented Lead-Acid Storage Batteries for Nuclear Power Plants” (Reference 3-74), which endorses IEEE 535 “IEEE Standard for Qualification of Class 1E Vented Lead Acid Storage Batteries for Nuclear Power Generating Stations,” (Reference 3-75).
- RG 1.40 “Qualification of Continuous Duty Safety-Related Motors for Nuclear Power Plants,” (Reference 3-76), which endorses IEEE 334, “IEEE Standard for Qualifying Continuous Duty Class 1E Motors for Nuclear Power Generating Stations,” (Reference 3-77) if considered applicable to BWRX-300 design.
- RG 1.63 “Electric Penetration Assemblies in Containment Structures for Nuclear Power Plants,” (Reference 3-78), which endorses IEEE 317, “IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations,” (Reference 3-79).
- RG 1.73 “Qualification Tests for Safety-Related Actuators in Nuclear Power Plants,” (Reference 3-80), which endorses IEEE 382, “IEEE Standard for Qualification of Safety-Related Actuators for Nuclear Power Generating Stations and Other Nuclear Facilities,” (Reference 3-81).
- RG 1.89 “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants” (Reference 3-68) which endorses IEC/IEEE-60780-323 (Reference 3-56) that includes IEEE 638 “IEEE Standard for Qualification of Class 1E Transformers for Nuclear Power Generating Stations,” (Reference 3-82).
- RG 1.213 “Qualification of Safety-Related Motor Control Centers for Nuclear Power Plants,” (Reference 3-83), considers conformance with the requirements of IEEE 649, “IEEE Standard for Qualifying Class 1E Motor Control Centers for Nuclear Power Generating Stations,” (Reference 3-84) if considered applicable to BWRX-300 design.
- RG 1.210 “Qualification of Safety-Related Battery Chargers and Inverters for Nuclear Power Plants,” (Reference 3-85), which endorses IEEE 650 “IEEE Standard for Qualification of Class 1E Static Battery Chargers, Inverters, and Uninterruptible Power Supply Systems for Nuclear Power Generating Stations,” (Reference 3-86).

Instrumentation and Control Equipment

Additional qualification guidance is considered for specific I&C equipment, if applicable, as follows:

- Control boards, panels, and racks classified as SC1 components – IEEE 420 (Reference 3-59) for their qualification program.

Qualification of computer based I&C systems is in accordance IEEE 7-4.3.2 “IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations,” (Reference 3-88). The EMC requirements are specified in RG 1.180 (Reference 3-72), IEEE 7-4.3.2 does not directly address RG 1.180 although the guidance in the RG is considered for I&C equipment.

When computer based I&C systems environmental type testing is performed:

- The system under test demonstrates that it functions and performs with safety software that has been validated and verified and is representative of the software to be installed in service.

- The testing demonstrates performance of all safety function that affected by environmental factors under the environmental service conditions specified in the design specification. Software algorithms, which are tested during Verification and Validation (V&V) testing, are not tested unless their outputs exercise different hardware components which are affected impacted by environmental conditions.
- The testing exercises all portions of the system that are necessary to accomplish the safety functions and those portions whose operation or failure could impair the safety functions.
- The testing confirms the response of digital interfaces and verifies that the design accommodates the potential effect of environmental conditions on the overall response of the system.

When computer based I&C systems environmental type testing is performed, the testing of a complete system is preferred. When testing of a complete system is not practical, confirmation of the dynamic response to the most limiting environmental and operational conditions is based on type testing of the individual modules and analysis of the cumulative effects of environmental and operational stress on the entire system to demonstrate required safety performance.

Cables, Raceways, Supports

For qualification of SC1 cables, the qualification guidance provided in IEEE 383 (Reference 3-60), and IEEE 384 (Reference 3-61) are considered. The test requirement guidance provided in IEEE 1202 (Reference 3-62) is used as a qualification program.

Seismic Category I supports (hangers) that support trays or conduit that carry SC1 circuits are designed and analysed to demonstrate qualification in accordance with IEEE (Reference 3-63).

Seismic Category II supports used for SCN raceway (conduit and cable tray) in Seismic Category I and II structures are analysed to withstand the effects of an SSE.

SC1 connection assemblies consider the qualification guidance provided in IEEE 572 (Reference 3-64) as endorsed by RG 1.156, “Qualification of Connection Assemblies for Production and Utilization Facilities”.

Line Mounted Equipment

Guidance in IEC/IEEE 60980-344, “IEEE/IEC International Standard-Nuclear Facilities Equipment Important to Safety-Seismic Qualification” (Reference 3-57) identifies that special consideration is required for line-mounted (pipe-supported) equipment regarding seismic qualification as the most critical seismic loading condition that occurs as a result of the piping or duct system. Guidance and further clarification for special considerations for line-mounted equipment is provided in IEEE 382 (Reference 3-65). Line mounted equipment also includes active mechanical equipment subjected to ASME QME-1 (Reference 3-58) including the Non-Mandatory Appendix QR-A.

3.9.4 Electromagnetic Compatibility

Accepted industry codes and standards are applied to establish an electromagnetic compatible environment applicable to electrical and I&C equipment. EMC qualification involves two elements:

1. Testing to assess susceptibility of equipment to interference levels that bound the expected electromagnetic environment.

2. Testing to assess emissions of equipment to ensure that the contribution to the electromagnetic environment does not invalidate representative interference levels applied for susceptibility testing.

Susceptibility testing allows assessment of equipment immunity to EMI/RFI and confirmation of its Surge Withstand Capability. Emissions testing provide assurance that equipment is compatible with the expected electromagnetic environment

.

3.10. Inservice Monitoring, Tests, Maintenance, and Inspections

3.10.1 Safety Design Bases and Requirements

NEDC-34176P (Reference 3-13) provides the specific features of the inspections, tests, modelling, and monitoring programs for the BWRX-300 plant.

SSCs that have a shorter service lifetime than the plant lifetime will be identified and described in the design documentation.

Design requirements associated with In-Service Monitoring, Tests, Maintenance, and Inspections involve accessibility, risk reduction, aging management, and easy-removable insulation for inspection, testing and maintenance.

In cases where SSCs are of SC and cannot be designed to support the desirable testing, inspection, or monitoring schedules, one of the following approaches shall be taken:

- Proven alternative methods, such as surveillance of reference items or use of verified and validated calculation methods, shall be specified
- Conservative safety margins shall be applied, or other appropriate precautions shall be taken, to compensate for possible unanticipated failures

3.10.2 Inservice Monitoring

The BWRX-300 levels of in-service monitoring for SSCs is related to the D-in-D DLs that are specified in Section 3.1.7 and associated classifications of SSCs in Section 3.2.2. Specifics on in-service monitoring are developed in the other PSR chapters. The design provides facilities for monitoring chemical conditions of fluids and of metallic and non-metallic materials.

3.10.3 Inservice Testing

In-service testing of certain ASME BPVC Section III, “Rules for Construction of Nuclear Facility Components,” (Reference 3-89) Division 1 pumps, valves, and snubbers (dynamic restraints) as applicable is performed in accordance with the ASME Operations and Management of Nuclear Power Plants (OM) code. In addition, in-service testing is performed in accordance with applicable IAEA Safety Standards.

Pre-service test results will be documented and used as a baseline for periodic in-service testing.

The design of BWRX-300 structures, systems and components provides access for the performance of in-service testing to the extent practicable.

The in-service testing program includes periodic tests and inspections that demonstrate the operational readiness of certain SSCs that perform a function in shutting down the reactor to a safe shutdown condition, maintaining a safe shutdown condition, or mitigating the consequences of an accident. Specific required in-service tests are established in other PSR chapters, but periodic and ISI and testing are established for:

- Nuclear pressure boundary components
- Containment components
- Containment structures
- Safety-related structures
- Balance-of-plant pressure boundary SC components or based on Aging Management requirements

3.10.4 Inservice Maintenance

Maintenance of the BWRX-300 Nuclear Power plant is based in part on the recommendations of the following publications:

- IAEA TECDOC-658, “Safety Related Maintenance in the Framework of the Reliability Centered Maintenance Concept,” (Reference 3-90)
- IAEA Safety Standards Series, No. NS-G-2.6, “Maintenance, Surveillance and ISI in Nuclear Power Plants,” (Reference 3-91)
- IAEA Safety Standards Series – GSR Part 2: “The Management System for Facilities and Activities,” (Reference 3-92)

Baseline data will be gathered during initial testing and system commissioning of SSCs.

NEDC-34176P (Reference 3-13) provides programmatic requirements for in service maintenance.

3.10.5 Inservice Inspection

Mechanical components and equipment including heat exchangers, pipe supports, pumps, valves, and vessels, that are classified as ASME BPVC Division 1 Class 1, 2 or 3 are designed and provided with accessible openings for ISI and testing, to justify the operational readiness of components and equipment as set forth within ASME BPVC III-Division 1.

Components and equipment, that require inspections and testing to satisfy ASME BPVC-XI-Division 1 requirements, are examined by appropriate ISI, and testing techniques, including ASME BPVC III Division 1 and ASME Code OM prior to the component or equipment leaving the manufacturer’s facility.

Non-Destructive Examination (NDE) methods are described within ASME BPVC-V and ASME BPVC-XI.

Component and equipment procurement specifications provide detailed requirements, which are to be used during the manufacturing phase and installation at the plant site.

NEDC-34176P (Reference 3-13) provides programmatic requirements for ISIs.

3.11. Compliance with National and International Standards

The specific PSR chapters provide prescriptive details that related to the BWRX-300 design features and their alignment with regulations including compliance with both national and international standards. PSR Ch. 3 forms the majority of requirements for other chapters used in the design of the BWRX-300 new nuclear plant.

3.11.1 Claims, Arguments, and Evidence Structure

Expectations

The "ONR Safety Assessment Principles (SAPs) for Nuclear Facilities," (Reference 3-93) identify ONR's expectation that a safety case should clearly set out the trail from safety claims, through arguments to evidence. This approach can be given as:

- **Claims** (assertions) are statements that indicate why a facility is safe
- **Arguments** (reasoning) explains the approaches to satisfying the claims
- **Evidence** (facts) supports and forms the basis (justification) of the arguments

Approach

GEH has structured its submission using the 'Claims, Arguments and Evidence', or CAE, approach that has been widely used in the licensing of recent nuclear power projects in the UK. The top-level claim, referred to as the Fundamental Objective, is provided below:

> **Fundamental Objective**
>
> The BWRX-300 is capable of being constructed, operated, and decommissioned in accordance with the standards of environmental, safety, security and safeguard protection required in the UK.

The Fundamental Objective is supported by the following Level 1 Claim for the PSR:

> **Level 1 Claim:**
>
> The safety risks to workers and the public during the construction, commissioning, operation and decommissioning of the BWRX-300 have been reduced as low as reasonably practicable (ALARP).

This is in turn supported by the following Level 2 Claims:

> **Level 2 Claims:**
>
> The functions of systems and structures have been derived and substantiated taking into account RGP and OPEX, and processes are in place to maintain these through-life (Engineering Analysis).
>
> The BWRX-300 has been developed in accordance with approved procedures, with appropriate governance and assurance arrangements by a competent and clearly defined organisation (Safety Case Area).
>
> A suitable and sufficient safety analysis has been undertaken which presents a comprehensive fault and hazard analysis that specifies the requirements on the safety measures and informs emergency arrangements (Safety Analysis).
>
> Safety risks have been reduced as low as reasonably practicable.

These claims are then further subdivided and supported by arguments and evidence within the PSR chapters, although aspects of the evidence will only come available once the BWRX-300 enters the detailed design phase during site-specific licensing.

3.11.2 Numerical Targets

The ONR SAPs (Reference 3-93) introduce numerical targets that the ONR uses in assessing the acceptability of a facility or activity. These are provided in Appendix C.

It is the intention that in the next licensing phase, a set of numerical targets will be established that are based on the targets presented in the ONR SAPs. The general principle will be to establish targets equivalent to the Basic Safety Level provided by the SAPs along with the requirement that risks are ALARP. This is captured as a Forward Action Plan item shown in Appendix B.

3.11.3 Categorisation and Classification

The BWRX-300 approach to categorisation and classification has been described in Section 3.2. The ONR SAPs (Reference 3-93) set out UK regulatory expectations for categorisation and classification, with this being discussed in Appendix C.

It has been identified that there is no provision in the BWRX-300 approach to categorisation of safety functions to assign a normal operation safety function to anything other than Safety Category 3, other than in the case where the failure of the associated SSC has been demonstrated to be practically eliminated. A Forward Action Plan item has been raised to address this, as discussed further in Appendix C.

Table 3-1: Identification of Defence Levels

Level of Defence/DL	Objective	Design Means	Operational Means
Level 1/DL1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures
Level 2/DL2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features (Safety Category 3)	Abnormal operating procedures/emergency operating procedures
Level 3/DL3	Control of design basis accidents	Engineered safety features (Safety Category 1)	Emergency operating procedures
Level 4a/DL4a	Control of DECs to prevent core melt	Safety features for DECs without core damage (Safety Category 2)	Emergency operating procedures
Level 4b/DL4b	Control of DECs to prevent or mitigate the consequences of severe accidents	Safety features for DECs with core damage (Safety Category 3)	Complementary emergency operating procedures/severe accident management guidelines
Level 5/DL5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans

Table 3-2: Safety Category for Functions Based on Defence Line Assignment

Safety Category	Defence Line 3 Functions	Defence Line 4a Functions	Defence Line 2/4b Functions	Normal Functions
1	Primary function Integral support functions			
2	• Post 72-hour primary and support functions	Primary function Integral support functions Post 72-hour primary and support functions		
3	• Post 7-day primary and support functions • Make-ready support functions	• Post 7-day primary and support functions • Make-ready support functions	Primary function Integral support functions Post 72-hour primary and support functions Post 7-day primary and support functions	• Normal functions that perform a fundamental safety function • Normal functions that maintain the reactor parameters
N			• Make-ready support functions	• Make-ready support functions

Table 3-3: Codes and Standards for Pressure-Retaining Equipment

Quality Group	ASME BPVC Section III Code Classes	Pressure Vessels and Heat Exchangers[4]	Pipes, Valves, and Pumps	Storage Tanks 0-103 kPaG (0-15 psig)	Storage Tanks Atmospheric	ASME BPVC Section III Component Supports	Non-ASME BPVC Section III Component Supports	Core Support Structures and Reactor Internals	Containment Boundary
A	1	NCA and NB	NCA and NB	—	—	NCA and NF	—	—	—
B	2	NCA and NCD	NCA and NCD	NCA and NCD	NCA and NCD	NCA and NF	—	—	—
	MC	—	—	—	—	—	—	—	NCA and NE [1]
	CS	—	—	—	—	—	—	NCA and NG	—
C	3	NCA and NCD	NCA and NCD	NCA and NCD	NCA and NCD	NCA and NF	—	—	—
D	—	ASME BPVC Sect. VIII Division 1	ASME B31.1 for piping and valves[2]	API 620 or equivalent [3]	API 650 AWWA D100-11 ASME B96.1 or equivalent[3]	—	Manufacturer Specified Standards, e.g., ASME B31.1, AISC	—	—

Notes:

(1) Excluding the Steel-Plate Composite Containment Vessel (SCCV).

(2) For pumps classified in Quality Group D, the ASME BPVC, Section VIII, Division 1 is used as a guide in determining the wall thickness for pressure retaining parts and in sizing the cover bolting.

(3) Tanks are designed to meet the intent of American Petroleum Institute (API) Standard 620, “Design and Construction of Large, Welded, Low-Pressure Storage Tanks,” (Reference 3-49), API 650, “Welded Steel Tanks for Oil Storage,” (Reference 3-50), American Water Works Association (AWWA), “Welded Carbon Steel Tanks for Water Storage,” (Reference 3-51), and/or ASME B96.1 standards, “Welded Aluminum-Alloy Storage Tanks,” (Reference 3-52), as applicable.

(4) For Tubular Exchanger Manufacturers Association (TEMA)-style heat exchangers, both the ASME Code and TEMA standard, “Standards of the Tubular Exchanger Manufacturers Association,” (Reference 3-53) are considered. Other heat exchanger design styles/configurations are not subject to the TEMA standard.

(5) Acronyms used in Table 3-3 refer to the ASME BPVC “Section III – Rules for Constructions of Nuclear Facility Components,” (Reference 3-54) subsections as follows:

- Subsection NCA - General Requirements for Division 1 and Division 2.
- Division 1 Subsections:
  - Subsection NB – Class 1 Components
  - Subsection NCD – Class 2 and 3 Components
  - Subsection NE - Metal Containment (MC)
  - Subsection NF – Supports
  - Subsection NG – Core Support Structure (CS)

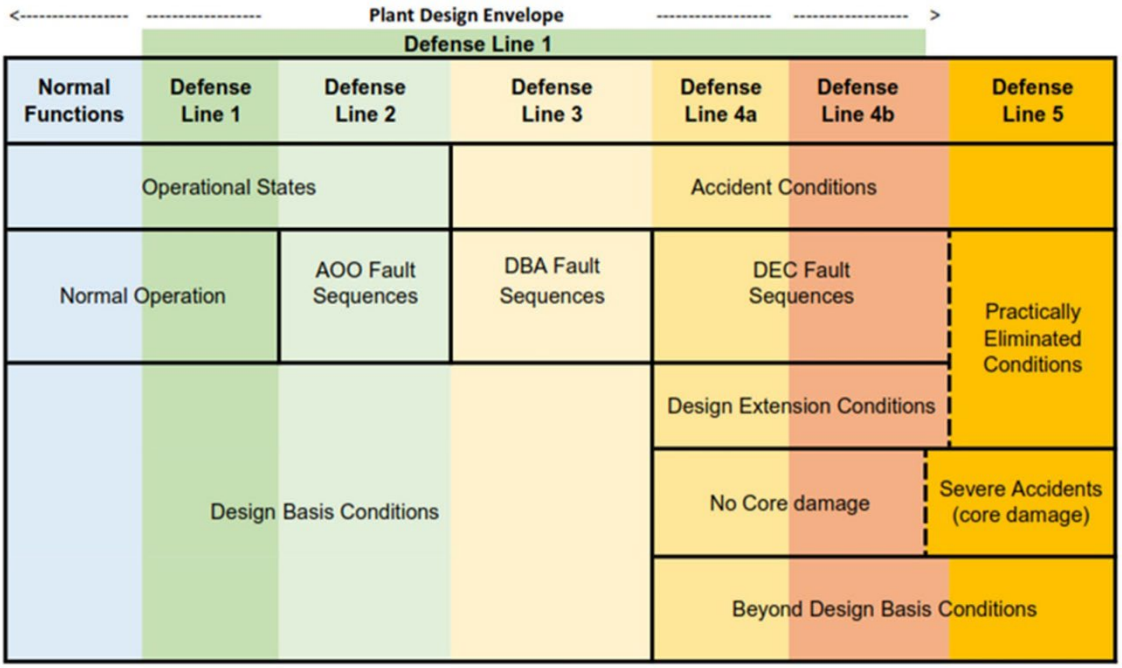

Figure 3-1: Defence-in-Depth - Plant States and Defence Lines

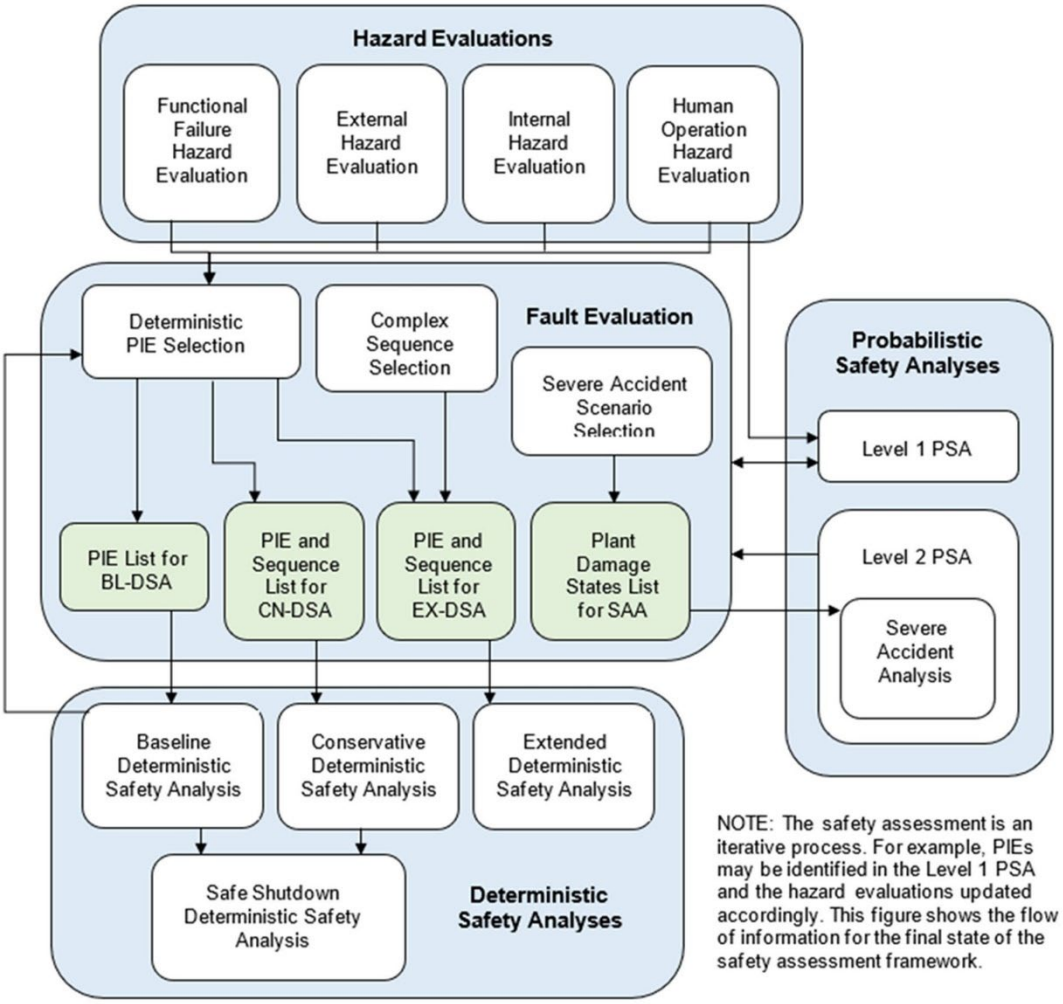

Figure 3-2: BWRX-300 Safety Strategy Implementation Process

3.12. References

3-1 NEDC-34165P, “BWRX-300 UK GDA Ch. 3: Safety Objectives and Design Rules for SSCs (Attachment 1),” GE-Hitachi Nuclear Energy, Americas, LLC.

3-2 IAEA No. SSG-61, “IAEA Safety Standards – Format and Content of the Safety Analysis Report for Nuclear Power Plants,” International Atomic Energy Agency. 2021.

3-3 NEDC-34166P, “BWRX-300 UK GDA Ch. 4: Reactor (Fuel and Core),” GE-Hitachi Nuclear Energy, Americas LLC.

3-4 NEDC-34167P, “BWRX-300 UK GDA Ch. 5: Reactor Coolant System and Associated Systems, GE-Hitachi Nuclear Energy, Americas, LLC.

3-5 NEDC-34168P, “BWRX-300 UK GDA Ch. 6: Engineered Safety Systems,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-6 NEDC-34169P, “BWRX-300 UK GDA Ch. 7: Instrumentation and Control,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-7 NEDC-34170P, “BWRX-300 UK GDA Ch. 8: Electrical Power,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-8 NEDC-34171P, “BWRX-300 UK GDA Ch. 9A: Auxiliary Systems,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-9 NEDC-34172P, “BWRX-300 UK GDA Ch. 9B: Civil Structures,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-10 NEDC-34173P, “BWRX-300 UK GDA Ch. 10: Steam and Power Conversion Systems,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-11 NEDC-34174P, “BWRX-300 UK GDA Ch. 11: Management of Radioactive Waste,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-12 NEDC-34175P, “BWRX-300 UK GDA Ch. 12: Radiation Protection,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-13 NEDC-34176P, “BWRX-300 UK GDA Ch. 13: Conduct of Operations,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-14 NEDC-34177P, “BWRX-300 UK GDA Ch. 14: Plant Construction and Commissioning,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-15 NEDC-34178P, “BWRX-300 UK GDA Ch.15: Safety Analysis (Including Fault Studies, PSA, and Hazard Assessment),” GE-Hitachi Nuclear Energy, Americas, LLC.

3-16 NEDC-34179P, “BWRX-300 UK GDA Ch. 15.1: Safety Analysis: General Considerations,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-17 NEDC-34180P, “BWRX-300 UK GDA Ch. 15.2: Safety Analysis: ID, Categorisation and Grouping of PIEs and Accident Scenarios,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-18 NEDC-34181P, “BWRX-300 UK GDA Ch. 15.3: Safety Analysis: Safety Objective and Acceptance Criteria,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-19 NEDC-34182P, “BWRX-300 UK GDA Ch. 15.4: Safety Analysis: Human Actions,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-20 NEDC-34184P, “BWRX-300 UK GDA Ch. 15.5: Safety Analysis: Deterministic Safety Analyses,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-21 NEDC-34184P, “BWRX-300 UK GDA Ch. 15.6: Safety Analysis: Probabilistic Safety Assessment,” GE-Hitachi Nuclear Energy Americas, LLC.

3-22 NEDC-34185P, “BWRX-300 UK GDA Ch. 15.7: Safety Analysis: Internal Hazards,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-23 NEDC-34186P, “BWRX-300 UK GDA Ch. 15.8: Safety Analysis: External Hazards,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-24 NEDC-34187P, “BWRX-300 UK GDA Ch. 15.9: Safety Analysis: Summary of the Results of the Safety Analyses (Including Fault Schedule),” GE-Hitachi Nuclear Energy, Americas, LLC.

3-25 NEDC-34188P, “BWRX-300 UK GDA Ch.16: Operational Limits and Conditions,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-26 NEDC-34189P, “BWRX-300 UK GDA Ch. 17: Management for Safety and Quality Assurance,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-27 NEDC-34190P, “BWRX-300 UK GDA Ch. 18: Human Factors Engineering,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-28 NEDC-34191P, “BWRX-300 UK GDA Ch. 19: Emergency Preparedness and Response,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-29 NEDC-34192P, “BWRX-300 UK GDA Ch. 20: Environmental Aspects,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-30 NEDC-34193P, “BWRX-300 UK GDA Ch. 21: Decommissioning and End of Life Aspects,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-31 NEDC-34194P, “BWRX-300 UK GDA Ch. 22: Structural Integrity,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-32 NEDC-34195P, “BWRX-300 UK GDA Ch. 23: Reactor Chemistry,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-33 NEDC-34196P, “BWRX-300 UK GDA Ch. 24: Conventional Safety and Fire Safety,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-34 NEDC-34197P, “BWRX-300 UK GDA Ch. 25: Security Annex,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-35 NEDC-34198P, “BWRX-300 UK GDA Ch. 26: Interim Storage of Spent Fuel,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-36 NEDC-34199P, “BWRX-300 UK GDA Ch.27: ALARP Evaluation,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-37 NEDC-34200P, “BWRX-300 UK GDA Ch. 28: Safeguards Annex,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-38 NEDC-33934P, “BWRX-300 Safety Strategy,” GE-Hitachi Nuclear Energy Americas, LLC, 2024.

3-39 IAEA Safety Standards Series No. SSR-2/1, “Safety of Nuclear Power Plants: Design,” International Atomic Energy Agency, Revision 1, Feb 2016.

3-40 IAEA Safety Standards Series No. SF-1, “Fundamental Safety Principles,” International Atomic Energy Agency, 2006.

3-41 INSAG-12. “Basic Safety Principles for Nuclear Power Plants 75-INSAG-3,” International Nuclear Safety Advisory Group. Revision 1. October 1999.

3-42 IEC 61513: 2011, 2nd Ed. “Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems,” International Electrotechnical Commission. August 2011.

3-43 006N2631 Rev 2. “I&C Plant Level Design Assurance Plan,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-44 006N9508 Rev 1. “BWRX-300 Program Configuration Management Implementation Plan,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-45 IAEA Safety Standards Series No. SSG-30, “Safety Classification of Structures, Systems and Components in Nuclear Power Plants,” International Atomic Energy Agency, May 2014.

3-46 USNRC Regulatory Guide 1.143, “Design Guidance for Radioactive Waste Management Systems, Structures, and Components Installed in Light-Water-Cooled Nuclear Power Plants,” US Nuclear Regulatory Commission, Revision 2, November 2001.

3-47 ASCE/SEI 43-19, “Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities,” American Society of Civil Engineers, 2020.

3-48 USNRC Regulatory Guide 1.26, “Quality Group Classifications and Standards for Water-Steam and Radioactive-Waste-Containing Components of Nuclear Power Plants,” US Nuclear Regulatory Commission, Revision 5, February 2017.

3-49 API 620, “Design and Construction of Large, Welded, Low-Pressure Storage Tanks,” American Petroleum Institute, Twelfth Edition, April 2018.

3-50 API 650, “Welded Steel Tanks for Oil Storage,” American Petroleum Institute, Thirteenth Edition, January 2021.

3-51 AWWA D100-11, “Welded Carbon Steel Tanks for Water Storage,” American Water Works Association, July 2011.

3-52 ASME B96.1, “Welded Aluminum-Alloy Storage Tanks,” American Society of Mechanical Engineers, 1999.

3-53 TEMA, “Standards of the Tubular Exchanger Manufacturers Association,” Tubular Exchanger Manufacturers Association, Tenth Edition, 2020.

3-54 ASME Boiler and Pressure Vessel Code, “Section III – Rules for Constructions of Nuclear Facility Components,” American Society of Mechanical Engineers, 2023 Edition.

3-55 NEDC-34164P, “BWRX-300 UK GDA Ch. 2: Site Characteristics,” GE-Hitachi Nuclear Energy, Americas, LLC.

3-56 IEC/IEEE 60780-323, “Nuclear facilities – Equipment important to safety – Qualification,” International Electrotechnical Commission/ Institute of Electrical and Electronic Engineers.

3-57 IEC/IEEE 60980-344, “Nuclear facilities – Equipment important to safety –Seismic Qualification,” International Electrotechnical Commission/ Institute of Electrical and Electronic Engineers.

3-58 ASME QME-1, “Qualification of Active Mechanical Equipment Used in Nuclear Facilities,” American Society of Mechanical Engineers, 2021 Edition.

3-59 IEEE 420, “IEEE Standard for Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2023.

3-60 IEEE 383, “IEEE Standard for Qualifying Electric Cables and Splices for Nuclear Facilities,” Institute of Electrical and Electronics Engineers, 2023.

3-61 IEEE 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits,” Institute of Electrical and Electronics Engineers, 2018.

3-62 IEEE 1202, “IEEE Standard for Flame-Propagation Testing of Wire and Cable,” Institute of Electrical and Electronics Engineers, 2006.

3-63 IEEE 628, “IEEE Standard Criteria for the Design, Installation, and Qualification of Raceway Systems for Class 1E Circuits for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2020.

3-64 IEEE 572, “IEEE Standard for Qualification of Class 1E Connection Assemblies for Nuclear Power Generating Stations and Other Nuclear Facilities,” Institute of Electrical and Electronics Engineers, 2019.

3-65 IEEE 382, “IEEE Standard for Qualification of Safety-Related Actuators for Nuclear Generating Stations and Other Nuclear Facilities,” Institute of Electrical and Electronics Engineers, 2019.

3-66 IEEE 497 “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2016. (IEC 63147:2017/IEEE 497-2016).

3-67 Regulatory Guide 1.97. “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission. Revision 5. April 2019.

3-68 Regulatory Guide 1.89. “Environment Qualification of Certain Electric Equipment Important to Safety for Nuclear Plants,” U.S. Nuclear Regulatory Commission. Revision 2. May 2023.

3-69 EPRI TR-102323, “Guidelines for Electromagnetic Compatibility Testing of Power Plant Equipment,” Electric Power Research Institute, 2019.

3-70 MIL-STD-461G, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,” US Department of Defense, 2015.

3-71 IEC-62003, “Nuclear Power Plants – Instrumentation, Control, and Electrical Power Systems – Requirements for Electromagnetic Compatibility Testing,” International Electrotechnical Commission, 2020.

3-72 Regulatory Guide 1.180. “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” U.S. Nuclear Regulatory Commission. Revision 2. December 2019.

3-73 ASME BPVC, Section III, “Rules for Construction of Nuclear Facility Components - Appendices,” American Society of Mechanical Engineers, 2021 Edition.

3-74 Regulatory Guide 1.158. “Qualification of Safety-Related Vented Lead-Acid Storage Batteries for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission. Revision 1. March 2018.

3-75 IEEE 535, “IEEE Standard for Qualification of Class 1E Vented Lead Acid Storage Batteries for Nuclear Power Generating Stations,” Institute of Electrical and Electronic Engineers, 2022.

3-76 Regulatory Guide 1.40. “Qualification of Continuous Duty Safety-Related Motors for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission. Revision 1. February 2010.

3-77 IEEE 334, “IEEE Standard for Qualifying Continuous Duty Class 1E Motors for Nuclear Power Generating Stations,” Institute of Electrical and Electronic Engineers, 2006.

3-78 Regulatory Guide 1.63. “Electric Penetration Assemblies in Containment Structures for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission. Revision 3. February 1987.

3-79 IEEE 317, “IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Power Generating Stations,” Institute of Electrical and Electronic Engineers, 2013.

3-80 Regulatory Guide 1.73. “Qualification of Safety-Related Actuators in Production and Utilization Facilities,” U.S. Nuclear Regulatory Commission. Revision 2. January 2024.

3-81 IEEE 382, “IEEE Standard for Qualification of Safety-Related Actuators for Nuclear Power Generating Stations and Other Nuclear Facilities,” Institute of Electrical and Electronic Engineers, 2019.

3-82 IEEE 638, “IEEE Standard for Qualification of Class 1E Transformers for Nuclear Power Generating Stations,” Institute of Electrical and Electronic Engineers, 2013.

3-83 Regulatory Guide 1.213. “Safety-Related Motor Control Centers for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission. May 2009.

3-84 IEEE 649, “IEEE Standard for Qualifying Class 1E Motor Control Centers for Nuclear Power Generating Stations,” Institute of Electrical and Electronic Engineers, 2006.

3-85 Regulatory Guide 1.210. “Qualification of Safety-Related Battery Chargers and Inverters for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission. June 2008.

3-86 IEEE 650, “IEEE Standard for Qualification of Class 1E Static Battery Chargers and Inverters for Nuclear Power Generating Stations,” Institute of Electrical and Electronic Engineers, 2006.

3-87 Regulatory Guide 1.156. “Qualification of Connection Assemblies for Production and Utilization Facilities,” U.S. Nuclear Regulatory Commission. Revision 2. February 2023.

3-88 IEEE 7-4.3.2, “IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronic Engineers, 2016.

3-89 ASME BPVC, Section III, “Rules for Construction of Nuclear Facility Components,” Edition 2021, Subsection NCA, “General Requirements for Division 1 and Division 2,” American Society of Mechanical Engineers.

3-90 IAEA TECDOC-658, “Safety Related Maintenance in the Framework of the Reliability Centered Maintenance Concept,” International Atomic Energy Agency. Vienna, 1992.

3-91 IAEA Safety Standards Series, No. NS-G-2.6, “Maintenance, Surveillance, and Inservice Inspection in Nuclear Power Plants,” International Atomic Energy Agency.

3-92 IAEA Safety Standards Series – GSR Part 2: “The Management System for Facilities and Activities,” International Atomic Energy Agency.

3-93 “ONR Safety Assessment Principles for Nuclear Facilities,” 2014 Edition. Office for Nuclear Regulation. Revision 1. 2020.

3-94 NEDC-34140P Rev 03. “BWRX-300 Safety Case Development Strategy,” May 2024.

3-95 “The Health and Safety at Work etc. Act”, 1974.

3-96 ONR Nuclear Technical Assessment Guide NS-TAST-GD-094, Revision 2. “Categorisation of Safety Functions and Classification of Structures, Systems and Components,” Office for Nuclear Regulation. 2019.

3-97 NEDC-34161P, Rev 0. “Comparison of BWRX-300 Approach to Categorisation & Classification with UK Expectations,” September 2024.

APPENDIX A CLAIMS, ARGUMENTS AND EVIDENCE

A.1 Claims, Arguments, Evidence (CAE)

The ONR Safety Assessment Principles (SAPs) (Reference 3-93) identify ONR's expectation that a safety case should clearly set out the trail from safety claims, through arguments to evidence. The CAE approach can be explained as follows:

- Claims (assertions) are statements that indicate why a facility is safe
- Arguments (reasoning) explain the approaches to satisfying the claims
- Evidence (facts) supports and forms the basis (justification) of the arguments

The GDA CAE structure is defined within NEDC-34140P "BWRX-300 Safety Case Development Strategy," (SCDS) (Reference 3-94) and is a logical breakdown of the overall claim that:

> *"The BWRX-300 is capable of being constructed, operated and decommissioned in accordance with the standards of environmental, safety, security and safeguard protection required in the UK".*

This overall claim is broken down into Level 1 claims relating to environment, safety, security, and safeguards, which are then broken down again into Level 2 area related sub-claims and then finally into Level 3 (chapter level sub-claims).

The Level 3 sub-claims that PSR Ch. 3 demonstrates are identified within NEDC-34140P (Reference 3-94) and are as follows:

> *2.1.1: The safety functions (Design Basis) have been derived for the system/structure through a robust analysis, based upon RGP.*
>
> *2.1.3: The system/structure design has been undertaken in accordance with relevant design codes and standards (RGP) and design safety principles and taking account of OPEX to support reducing risks ALARP.*
>
> *2.1.4: System/structure performance will be validated by suitable testing throughout manufacturing, construction, and commissioning.*
>
> *2.1.5: Aging and degradation mechanisms will be identified and assessed in the design. Suitable examination, inspection, maintenance, and testing will be specified to maintain systems/structures fit-for-purpose through-life.*
>
> *2.4.1: RGP has been taken into account across all disciplines.*
>
> *2.4.2: OPEX and Learning from Experience (LfE) has been taken into account across all disciplines.*
>
> *2.4.3: Optioneering (all reasonably practicable measure have been implemented to reduce risk).*

In order to facilitate compliance, demonstration against the above Level 3 sub-claims, PSR Ch. 3 has derived a suite of arguments that comprehensively explain how their applicable Level 3 sub-claims are met (see Appendix B).

It is not the intention to generate a comprehensive suite of evidence to support the derived arguments, as this is beyond the scope of GDA Step 2. However, where evidence sources are available, examples are provided.

A.2 Risk Reduction As Low As Reasonably Practicable

It is important to note that nuclear safety risks cannot be demonstrated to have been reduced ALARP within the scope of a two-step GDA. It is considered that the most that can be

realistically achieved is to provide a reasoned justification that the BWRX-300 Small Modular Reactor (SMR) design aspects will effectively contribute to the development of a future ALARP statement. In this respect, PSR Ch. 3 contributes to the overall future ALARP case by demonstrating that:

- The chapter-specific arguments derived may be supported by existing and future planned evidence sources covering the following topics:
  - RGP has demonstrably been followed
  - OPEX has been taken into account within the design process
  - All reasonably practicable options to reduce risk have been incorporated within the design
- It supports its applicable level 3 sub-claims, defined within NEDC-34140P (Reference 3-94).

Probabilistic safety aspects of the ALARP argument are addressed within NEDC-34178P (Reference 3-15).

Table A-1: Safety Objectives and Design Rules for SSCs Claims and Arguments

Level 3 Chapter Claim	Chapter 3 Argument	Sections and/or reports that evidence the arguments:
2.1 The functions of systems and structures have been derived and substantiated taking into account RGP and OPEX, and processes are in place to maintain these through-life. (Engineering Analysis).		
2.1.1: The safety functions (Design Basis) have been derived for the system/structure through a robust analysis, based upon RGP.	The BWRX-300 design has been assessed for development at Darlington, in Canada, and the Tennessee Valley, USA. It is designed based on US and Canadian nuclear regulatory requirements, along with international good practice. The UK BWRX-300 safety functions, and system/structure design are developed from these BWRX-300 principles with the consideration of UK context.	PSR Ch. 3, Section 3.1 – General Safety Design Basis
2.1.3: The system/structure design has been undertaken in accordance with relevant design codes and standards (RGP) and design safety principles and taking account of OPEX to support reducing risks ALARP.		PSR Ch. 3 – All sections.
2.14: System/structure performance will be validated by suitable testing throughout manufacturing, construction and commissioning.	The structural acceptance criteria for seismic category I structures have been considered and identified using good engineering practice guidance.	PSR Ch. 3, Section 3.5 – Design of Seismic Category I Structures
	The appropriate ASME Class has been considered in development of the test acceptance criteria for mechanical components.	PSR Ch. 3, Section 3.6 – Mechanical Systems and Components
2.15: Aging and degradation mechanisms will be identified and assessed in the design.	Aging management topics to be covered as a minimum in design documents have been identified.	PSR Ch. 3, Section 3.1.12 – Design Considerations for Aging Management

Level 3 Chapter Claim	Chapter 3 Argument	Sections and/or reports that evidence the arguments:
Suitable examination, inspection, maintenance and testing will be specified to maintain systems/structures fit-for-purpose through-life.	Aging and degradation considerations as part of equipment qualification by analysis or testing (or a combination) have been recognised.	PSR Ch. 3, Section 3.9 – Equipment Qualification
	In-service examination, inspection and testing requirements will be developed taking cognisance of regulatory requirements and RGP.	PSR Ch. 3, Section 3.10 – In-Service Monitoring, Tests, Maintenance, and Inspections.
	An effective maintenance, surveillance, inspection and testing; aging and degradation procedures can be developed to ensure the requirement of operating limits and conditions is effective.	PSR Ch. 3, Section 3.1.10 – Design Approaches for the Reactor Core and for Fuel Storage. PSR Ch. 3, Section 3.1.12 – Design Considerations for Aging Management. PSR Ch. 13, Section 13.3.2 – Maintenance, Surveillance, Inspection and Testing.
2.4: Safety risks have been reduced as low as reasonably practicable.		
2.4.1: RGP has been taken into account across all disciplines.	US and Canadian regulatory guidance, along with engineering good practice guidance, have been considered alongside the UK regulatory requirements.	PSR Ch. 3
2.4.2: OPEX and LfE has been taken into account across all disciplines.	OPEX has been considered from decommissioning of existing facilities and incorporation of this ensured at the design phase to best facilitate the learning.	PSR Ch. 3, Section 3.1.7 – Application of General Design Requirements and Technical Acceptance Criteria.
	The Safety Strategy principle for fuel handling and storage uses features proven through operating experience.	PSR Ch. 3, Section 3.1.10 – Design Approaches for the Reactor Core and for Fuel Storage.
	The seismic equipment qualification methodology has considered and made use of actual seismic experience, using external seismic experience databases.	PSR Ch. 3, Section 3.9.2 – Seismic and Dynamic Qualification of Mechanical and Electrical Equipment.

Level 3 Chapter Claim	Chapter 3 Argument	Sections and/or reports that evidence the arguments:
2.4.3: Optioneering (all reasonably practicable measures have been implemented to reduce risk).	RGP and guidance is considered as part of the selection process to ensure that the selected measure complies with the guidance.	PSR Ch. 3 – All Sections

APPENDIX B FORWARD ACTIONS

FAP No.	Finding	Forward Action Plan Item	Delivery Phase
PSR3-1	The BWRX-300 design has been developed with reference to USNRC guidance rather than UK-specific guidance.	Justification is required as to why design against USNRC requirements and guidance is appropriate for UK deployment and that its use is in line with Regulatory Good Practice. Alternative codes and standards also need to be considered where appropriate to the UK.	Completed within Step 2.
PSR3-2	Safety goals are currently set for the BWRX-300 target Core Damage Frequency and Large Release Frequency. Whilst these are useful metrics to assess, they do not allow comparison with the UK ONR SAP Numerical Targets 4-9 within the PSR.	Determine and justify the numerical targets to be adopted for the UK implementation of the BWRX-300 and document them in the specification for the safety case manual for implementation of the BWR-300 in the UK. Note: detailed methods development and performance of analysis will be in a later licensing phase.	Completed within Step 2.

APPENDIX C UK SPECIFIC CONTEXT INFORMATION

C.1 UK Context for Numerical Targets

C.1.1 ONR's Safety Assessment Principles and Numerical Targets

ONR's SAPs (Reference 3-93) introduce the numerical targets that ONR itself uses in assessing the acceptability of a facility or activity.

SAP NT.1 states:

> *Safety cases should be assessed against the SAPs numerical targets for normal operational, design basis fault and radiological accident risks to people on and off the site.*

ONR states in the SAPs that the targets should be used by inspectors *"… as an aid to judgement when considering whether radiological hazards are being adequately controlled and risks reduced to ALARP".*

Adding (para. 695):

> *The targets quantify ONR's risk policy and have been set to assist us in making proportionate regulatory decisions and targeting our resources to where the risks and hazards are greatest. More specifically, the targets are guides to inspectors to indicate where additional safety measures may need to be considered and, in the case of permissioning decisions, to help judge whether risks are tolerable.*

Normal operation – any person on the site	**Target 1**
The targets and a legal limit for effective dose in a calendar year for any person on the site from sources of ionising radiation are: Employees working with ionising radiation: BSL(LL): 20 mSv BSO: 1 mSv Other employees on the site: BSL: 2 mSv BSO: 0.1 mSv *Note that there are other legal limits on doses for specific groups of people, tissues and parts of the body (IRR17). Normal operational doses should also be reduced ALARP.*	

Normal operation – any group on the site	**Target 2**
The targets for average effective dose in a calendar year to defined groups of employees working with ionising radiation are: BSL: 10 mSv BSO: 0.5 mSv	

Normal operation – any person off the site	**Target 3**

The target and a legal limit for effective dose in a calendar year for any person off the site from sources of ionising radiation originating on the site are:

BSL(LL): 1 mSv
BSO: 0.02 mSv

Note that there are other legal limits to tissues and parts of the body (IRR17).

Design basis fault sequences – any person	**Target 4**

The targets for the effective dose received by any person arising from a design basis fault sequence are:

On site:

BSL: 20 mSv for initiating fault frequencies exceeding 1×10^{-3} pa
200 mSv for initiating fault frequencies between 1×10^{-3} and 1×10^{-4} pa
500 mSv for initiating fault frequencies between 1×10^{-4} and 1×10^{-5} pa

BSO: 0.1 mSv

Off site:

BSL: 1 mSv for initiating fault frequencies exceeding 1×10^{-3} pa
10 mSv for initiating fault frequencies between 1×10^{-3} and 1×10^{-4} pa
100 mSv for initiating fault frequencies between 1×10^{-4} and 1×10^{-5} pa

BSO: 0.01 mSv

Individual risk of death from accidents – any person on the site	**Target 5**

The targets for the individual risk of death to a person on the site, from accidents at the site resulting in exposure to ionising radiation, are:

BSL: 1×10^{-4} pa
BSO: 1×10^{-6} pa

Frequency dose targets for any single accident – any person on the site	**Target 6**

The targets for the predicted frequency of any single accident in the facility, which could give doses to a person on the site, are:

Effective dose, mSv	**Predicted frequency per annum**	
	BSL	**BSO**
2–20	1×10^{-1}	1×10^{-3}
20–200	1×10^{-2}	1×10^{-4}
200–2000	1×10^{-3}	1×10^{-5}
> 2000	1×10^{-4}	1×10^{-6}

Individual risk to people off the site from accidents	Target 7
The targets for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation, are: BSL: 1×10^{-4} pa BSO: 1×10^{-6} pa	

Frequency dose targets for accidents on an individual facility – any person off the site	Target 8
The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site are:	

Effective dose, mSv	Total predicted frequency per annum	
	BSL	BSO
0.1–1	1	1×10^{-2}
1–10	1×10^{-1}	1×10^{-3}
10–100	1×10^{-2}	1×10^{-4}
100–1000	1×10^{-3}	1×10^{-5}
>1000	1×10^{-4}	1×10^{-6}

Total risk of 100 or more fatalities	Target 9
The targets for the total risk of 100 or more fatalities, either immediate or eventual, from accidents at the site resulting in exposure to ionising radiation, are: BSL: 1×10^{-5} pa BSO: 1×10^{-7} pa	

ONR acknowledge in the SAPs that a safety case does not necessarily require detailed calculation for each target and that intermediate targets such as Core Damage Frequency (CDF) and Large Release Frequency (LRF) can be considered provided that *"…the overarching Principles EKP.1 to EKP.5 are not compromised through such approaches".*

As discussed in Section 3.1.3, the BWRX-300 has adopted stringent CDF and LRF targets of 1x10-6 per reactor-year and 1x10-7 per reactor-year respectively, along with the application of radiological protection principles to ensure that normal operational exposures reduced to levels that are ALARP.

C.1.2 Alignment of the BWRX-300 Safety Philosophy with ONRs Engineering Key Principles

The overarching Engineering Key Principles (EKPs) are listed below.

- EKP.1 (Inherent safety) - The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility
- EKP.2 (Fault tolerance) - The sensitivity of the facility to potential faults should be minimised
- EKP.3 (Defence in depth) - Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.

- EKP.4 (Safety function) - The safety function(s) to be delivered within the facility should be identified by a structured analysis
- EKP.5 (Safety measures) - Safety measures should be identified to deliver the required safety function(s)

The overall safety philosophy for the design of the BWRX-300 is referred to as the Safety Strategy NEDC-33934P (Reference 3-38). The Safety Strategy ensures a consistent, robust, and systematic design approach and provides a framework for comprehensive and systematic safety assessments of the design. This is accomplished through the application of Safety and Design Principles based on the principles set forth in the IAEA document SSR-2/1 (Reference 3-39).

The BWRX-300 safety objective is to achieve a design with a very high level of safety with Safety and Design Principles based on a D-in-D approach consisting of five levels of defence called DLs. Safety is enhanced by deliberate design decisions informed by deterministic and probabilistic safety analyses, through an iterative safety framework wherein the design is implemented to meet defined safety objectives, which are confirmed via safety assessments. Results of safety assessments then provide feedback regarding the design and the process is repeated as required.

Design robustness is incorporated through appropriate design margins, and via DiD by the introduction of passive safety features which do not require dependence on external sources of power or operator actions to perform their stipulated functions.

C.1.3 Approach to Numerical Targets for the Preliminary Safety Report

There is a strong alignment between the BWRX-300 safety philosophy and the EKPs. This gives confidence that the application of stringent intermediate CDF and LRF targets, combined with the radiological protection principles and safety strategy for the BWRX-300 will ensure that Legal Limits are met and that risks can be demonstrated to be tolerable and ALARP.

The PSR, therefore, will continue to adopt these intermediate targets and provide a demonstration of risk in the context of CDF and LRF.

C.1.4 Approach to Numerical Targets for a Future Licensing Phase

It is the intention that in the next licensing phase (development of either a UK generic PCSR or site specific PCSR) a set of numerical targets will be established that are based on targets 1 to 9 presented in the SAPs. The general principle will be to establish targets equivalent to the Basic Safety Limit (BSL) combined with the requirement for the risks to be ALARP; the requirement to demonstrate an ALARP position is the overriding requirement, regardless of the position against the BSL or Basic Safety Objective (BSO).

This intention is captured in Forward Action Plan items shown in Appendix B.

C.2 UK Context for ALARP

C.2.1 Legislative Basis for ALARP

The legislative basis of ALARP in the UK is derived from the “Health and Safety at Work etc. Act,” 1974 (Reference 3-95). The Act places duties on employers to ensure the health, safety, and welfare of their employees and to conduct their operations so that persons not in their employment are not exposed to risks to their health and safety. The employer is required to ensure that these duties are met So Far As Is Reasonably Practicable (SFAIRP), which is the basic legal requirement that each employer needs to conform to. In Office for Nuclear Regulation (ONR) guidance, the term ALARP is equivalent to SFAIRP.

C.2.2 ONR Safety Assessment Principles and ALARP

The ONR's Safety Assessment Principles (SAPs) for Nuclear Facilities (Reference 3-93), place the expectation that the safety case should provide an analysis of normal operation, potential faults and accidents, and of the engineering design and operations, and demonstrate the risks from all these perspectives have been reduced to ALARP.

The ALARP approach should include consideration of the following four aspects:

- Demonstration that international reactor OPEX has been taken into account in the overall design philosophy and in specific system designs
- Demonstration that RGP has been applied, including codes and standards comparison/justification
- Identification and evaluation of options (Optioneering)
- Risk assessment, as a way of understanding the significance of the issue to the holistic demonstration of ALARP i.e., to identify the severity of shortfalls against numerical targets, RGP, and/or deterministic rules

Following on from these is then the implementation of reasonably practicable improvements into the updated design reference.

In simple terms, the concept of ALARP is a requirement to take all measures to reduce risk where doing so is reasonably practicable. In most cases this is not done through an explicit comparison of costs and benefits, but rather by applying established RGP and standards. The development of RGP and standards includes ALARP considerations so in many cases meeting them is sufficient. In other cases, either where standards and RGP are less evident or not fully applicable, the onus is to implement measures to the point where the costs of any additional measures (in terms of money, time, or trouble – i.e., the sacrifice) would be grossly disproportionate to the further risk reduction that would be achieved (the safety benefit).

C.2.3 Approach to ALARP in the PSR

It is important to note that nuclear safety risks cannot be demonstrated to have been reduced ALARP within the scope of a PSR. It is considered that the most that can be realistically achieved is to provide a reasoned justification that the BWRX-300 SMR design aspects will effectively contribute to the development of a future ALARP demonstration.

The focus for the PSR, therefore, is to demonstrate that:

- operating experience has been taken into consideration
- the codes and standards used represent international Relevant Good Practice
- at a holistic level the fundamental design decisions made in the development of the BWRX-300 have the intent of reducing risks
- insights from the probabilistic risk analysis of previous generations of BWRs has been used to inform the BWRX-300 design

C.3 UK Context for Categorisation of Safety Functions and Classification of SSCs

C.3.1 ONR Safety Assessment Principles and Categorisation and Classification

UK regulatory expectations with respect to the categorisation of safety functions and classification of SSCs are set out in the Office for Nuclear Regulation's (ONR's) Safety Assessment Principles (SAPs) (Reference 3-93), with further guidance to inspectors provided in ONR Technical Assessment Guide 094 (TAG094), "Categorisation of Safety Functions and Classification of Structures, Systems and Components," (Reference 3-96). TAG094 contextualizes the categorization of safety functions and classification of SSCs as a key

activity in implementing a balanced approach to defence in depth in the design and operation of a nuclear facility, including Nuclear Power Plants (NPPs).

TAG094 sets out 5 high-level objectives for a scheme for categorization of safety functions and classification of SSCs:

- The systematic identification and categorisation of safety functions
- The systematic identification and classification of SSCs delivering those safety functions
- That the principle of D-in-D is applied, (with suitable and sufficient prevention, protection, and mitigation, in that order)
- That ALARP and RGP continue to always apply
- That classification informs the entire lifecycle of activities associated with SSCs

C.3.2 BWRX-300 Approach to Categorisation and Classification

The BWRX-300 schemes for the categorization of safety functions and the classification of SSCs are set out in Section 3.2.

The BWRX-300 approach to categorization of safety functions and classification of SSCs is based on the principles contained in IAEA SSR-2/1 (Reference 3-39) and IAEA SSG-30 (Reference 3-45). It can be summarized in three key steps:

- Functions that can impact nuclear safety are identified
- The identified functions are categorized (i.e., each assigned a safety category) based on their importance
- Safety classes are assigned to the components that perform the identified functions

In general, the approach provides a direct correlation between the DLs within which a safety function resides, which indicates its importance to safety, and its safety categorization, and then a direct linkage between the assigned safety categorization of a function and the classification of the SSC(s) through which it is delivered.

A specific review of the BWRX-300 approach to the categorization of safety functions and classification of SSCs against UK expectations has been performed and presented in NEDC-34161P, “Comparison of BWRX-300 Approach to Categorisation & Classification with UK Expectations,” (Reference 3-97).

This review shows that the BWRX-300 approach broadly aligns with UK expectations and meets the ONR’s 5 high-level objectives.

The review identified that there is a gap versus UK expectations with respect to normal operation safety functions:

- There is no provision in the BWRX-300 approach to categorization of safety functions to assign a normal operation safety function to anything other than Safety Category 3, other than in the case where the failure of the associated SSC has been demonstrated to be practically eliminated.

The potential impact of the identified gap has been considered and it is judged that based on more onerous reliability targets in BWRX-300 design compared with UK expectations and iterative confirmation of safety classifications as safety analysis progresses, there is confidence that the design of the BWRX-300 broadly aligns with UK expectations and will continue to do so.

There is judged to be no impact on the PSR, however closure of this gap will be required ahead of a future PCSR, and a Forward Action Plan item has been raised, as shown in NEDC-34161P (Reference 3-97).