HITACHI

GE Hitachi Nuclear Energy

NEDO-34184

Revision B

July 2025

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

BWRX-300 UK Generic Design Assessment (GDA) Subchapter 15.6 - Probabilistic Safety Assessment

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

INFORMATION NOTICE

This document does not contain proprietary information and carries the notation “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, UK EXPORT CONTROL 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) subchapter is to describe the development of the Probabilistic Safety Assessment (PSA) that has been undertaken to analyse the risk profile of the BWRX-300. An overview of the results is presented to demonstrate that the overall risk of core damage and large release is low.

The scope and level of detail in the PSA, and thus presented in this subchapter, is commensurate with the stage of design development and with a Step 2 Generic Design Assessment (GDA). A Level 1 PSA is presented for internal events in all modes of operation with a Level 2 PSA for full power. Full power hazard Level 1 PSAs, including internal fire, internal flooding, seismic, high wind, and heavy load drop have been developed, with some Level 2 analyses for certain hazards. A spent fuel pool PSA has also been produced and is discussed. The subchapter is supported by a summary report and methodology report, which go into more detail regarding the assumptions, input data, task outputs and analysis of the results.

At this stage a full As Low As Reasonably Practicable (ALARP) assessment is not possible as the full scope PSA is not yet complete. However, the subchapter demonstrates that the PSA results have been, and will continue to be, used to risk-inform and support design optioneering to ensure that the risk is ALARP. In addition, given the low risks calculated from the analysis to date, it is expected that the final risk results will continue to show the site risk to be very low relative to traditional safety goals and numerical targets.

The PSA is an iterative process and will continue to be developed as the design develops. 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. This includes the development of numerical dose and risk-based targets against which a full scope Level 3 PSA will be assessed.

ACRONYMS AND ABBREVIATIONS

Acronym	Explanation
ALWR	Advanced Light Water Reactor
API	Application Programming Interface
ASME/ANS	American Society of Mechanical Engineers/American Nuclear Society
ATWS	Anticipated Transient Without Scram
BE	Basic Event
BIS	Boron Injection System
BOC	Break Outside Containment
BOP	Balance of Plant
BWR	Boiling Water Reactor
CAFTA	Computer Aided Fault Tree Analysis
CCF	Common Cause Failure
CDF	Core Damage Frequency
CET	Containment Event Tree
COPS	Containment Overpressure Protection System
CRD	Control Rod Drive
CST	Condensate Storage Tank
DCIS	Distributed Control and Information System
DL	Defence Lines
DSA	Deterministic Safety Analyses
EME	Emergency Mitigating Equipment
EPRI	Electric Power Research Institute
ES	Event Sequence
FAP	Forward Action Plan
FDF	Fuel Damage Frequency
FLEX	Flexible Mitigation Capability
FMCRD	Fine Motion Control Rod Drive
FMEA	Failure Modes and Effects Analysis
FPC	Fuel Pool Cooling and Cleanup System
FPIE	Full Power Internal Events
FPS	Fire Protection System
FSF	Fundamental Safety Functions
FTREX	Fault Tree Reliability Evaluation Expert
FW	Feedwater
GDA	Generic Design Assessment
GEH	GE Hitachi Nuclear Energy
HCU	Hydraulic Control Unit

Acronym	Explanation
HEP	Human Error Probabilities
HFE	Human Failure Event
HRA	Human Reliability Analysis
HVS	Heating Ventilation and Cooling System
IAEA	International Atomic Energy Agency
ICS	Isolation Condenser System
IE	Initiating Event
ISLOCA	Interfacing Systems Loss of Coolant Accident
LLOCA	Large Loss of Coolant Accident
LOCA	Loss of Coolant Accident
LOPP	Loss of Preferred Power
LPSD	Low Power and Shutdown
LRF	Large Release Frequency
LWM	Liquid Waste Management
LWR	Light Water Reactor
MAAP	Modular Accident Analysis Program
MCC	Motor Control Centre
MCR	Main Control Room
MCS	Minimal Cutsets
MLOCA	Medium Loss of Coolant Accident
MOV	Motor Operated Valves
NBS	Nuclear Boiler System
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PAU	Physical Analysis Units
PCCS	Passive Containment Cooling System
PCER	Pre-Construction Environment Report
PCS	Power Conversion System
PCSR	Pre-Construction Safety Report
PCW	Plant Cooling Water
POS	Plant Operating State
PRA	Probabilistic Risk Analysis
PSA	Probabilistic Safety Assessment
PSR	Preliminary Safety Report
RAW	Risk Achievement Worth
RB	Reactor Building
RGP	Relevant Good Practice
RPS	Reactor Protection System

Acronym	Explanation
RPV	Reactor Pressure Vessel
RVR	Reactor Vessel Rupture
SA	Severe Accident
SAP	Safety Assessment Principles
SCR	Secondary Control Room
SDC	Shutdown Cooling
SFP	Spent Fuel Pool
SLOCA	Small Loss of Coolant Accident
SPD	Standard Plant Design
SPSA	Seismic Probabilistic Safety Assessment
SSC	Structures, Systems and Components
SSG	Specific Safety Guide
TB	Turbine Building
TRACG	Transient Reactor Analysis Code GEH
UPR	Ultimate Pressure Regulation
URD	Utility Requirements Document
USNRC	U.S. Nuclear Regulatory Commission
WSB	Wind Speed Bin

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
A	All	Initial Issuance
B	All	Update for end of GDA Step 2 consolidation

15.6 PROBABILISTIC SAFETY ASSESSMENT

Introduction

The purpose of this PSR subchapter is to describe the BWRX-300 PSA that has been undertaken to support the design development and provide risk insights.

The subchapter presents a level of detail commensurate with a Step 2 GDA and is structured in line with the high-level contents of the International Atomic Energy Agency (IAEA) Specific Safety Guide (SSG) 61. As such, it presents the general methodology that has been used for internal events Level 1 and Level 2 PSA across all modes. Hazards PSA is also discussed, noting that no site-specific external hazard prioritisation has yet been performed. Seismic and high wind PSAs that have been performed for North American sites have been presented in this subchapter to demonstrate the approach that will be used and to give an estimate of the potential risk presented by these hazards which, due to the conservative approaches applied, is likely to be bounding. Internal fire and flooding PSAs as well as heavy load drop PSA are also presented. In addition, a spent fuel pool PSA is presented.

The main results are reported in Sections 15.6.6 and 15.6.7 and the risk insights are discussed in Section 15.6.8.

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 (FAP), which includes future work commitments and recommendations for future work where ‘gaps’ to GDA expectations have been identified. This includes a Level 3 PSA and development of numerical targets that allow comparison to the Office for Nuclear Regulation (ONR) “Safety Assessment Principles for Nuclear Facilities,” (SAPs) (Reference 15.6-1) numerical dose and risk-based targets, which are out of scope for GDA Step 2.

This subchapter describes the scope, methodology, results, and design insights of the design-phase PSA performed for the BWRX-300. The risk assessment performed provides an understanding of sensitivities, areas of importance, system interactions and areas of uncertainty.

Interfaces with other Chapters

The probabilistic assessment forms a key part of the overall safety analysis performed for the BWRX-300. As such, there are interfaces with the other parts of the safety analysis described in PSR Chapter 15 and, where appropriate, these are cross referenced in the text.

- The safety strategy is described in NEDO-34179, “BWRX-300 UK GDA Subchapter 15.1: General Considerations of the BWRX-300 Safety Analysis,” (Reference 15.6-2)
- Safety goals are described in NEDO-34181, “BWRX-300 UK GDA Subchapter 15.3: Safety Objectives and Acceptance Criteria,” (Reference 15.6-3)
- A description of the work on human actions is described in NEDO-34182, “BWRX-300 UK GDA Subchapter 15.4: Human Actions,” (Reference 15.6-4)
- The deterministic approach to internal hazards is described in NEDO-34185, “BWRX-300 UK GDA Subchapter 15.7: Internal Hazards,” (Reference 15.6-5)
- The deterministic approach to external hazards is described in NEDO-34186, “BWRX-300 UK GDA Subchapter 15.8: External Hazards,” (Reference 15.6-6)
- Deterministic assessments, including the approach for severe accident analysis, are presented in NEDO-34183, “BWRX-300 UK GDA Subchapter 15.5: Deterministic Safety Analysis,” (Reference 15.6-7)

- The PSA numerical results are presented in NEDO-34187, "BWRX-300 UK GDA Subchapter 15.9: Summary of Results," (Reference 15.6-8).

This subchapter is supported by 006N2915, "BWRX-300 Standard Plant Probabilistic Safety Assessment Methodology," (Reference 15.6-9) and 008N9751, "UK BWRX-300 PSA Summary Report," (Reference 15.6-10). The PSA Methodology Report describes the methodology for the full scope PSA and the PSA Summary Report describes the work that has been done in more detail including key assumptions, input data, task outputs and analysis of the results. It also provides signposting to the supporting PSA documentation for each topic area.

General Approach

A principal element of the "BWRX-300 Safety Strategy," 006N5064 (Reference 15.6-11) is the development and results of a PSA. The PSA provides an integrated review of the plant design and operational safety. It complements the results of the Deterministic Safety Analyses (DSA).

The BWRX-300 Safety Strategy implements a multi-faceted approach to safety assessment and determination of the overall plant risk profile. The approach makes use of hazard evaluations, DSA, and PSA, as well as specifically targeted analysis techniques which provide a basis for a comprehensive set of "design-to-analysis" requirements. These requirements inform design development and modifications such that the design can be demonstrated to effectively satisfy analysis acceptance criteria and the plant safety goals. The PSA supports risk-informed design developments and, together with the DSA, is used to understand the overall risk and any dominant contributors to risk. The PSA is an essential tool to aid the understanding of the strengths and weaknesses of a design with complex systems and interdependencies.

As with the overall safety strategy implementation process, the safety evaluations and analyses are performed iteratively as the design and documentation are developed. These processes then implement required modifications and provide feedback to the next iteration of the evaluations and analyses.

Integration of the PSA with other design activities is described in 006N3139, "BWRX-300 Design Plan," (Reference 15.6-12) and set out in Figure 15.6- 1. The report shows how the PSA output (in partnership with deterministic analyses) provides input into the design, which then may have further impact on the PSA models. The interface of the PSA, with the rest of the safety case and safety analysis, is described in the PSA Safety Strategy, 006N5064 (Reference 15.6-11). This presents the common framework based on Defence-in-Depth (D-in-D) principles under which both the design basis and the safety analysis (deterministic and probabilistic) sit. It presents the fault evaluation process, which uses both deterministic and probabilistic inputs, resulting in the development of the fault list (this is discussed further in Subchapter 15.2).

The design phase PSA is updated as additional design and site-specific information becomes available for the operating license application and will be used to develop a site-specific PSA, which will reflect the final design of the as-built to-be-operated plant. This is accomplished by assessing design vulnerabilities and optimizing the design in real time.

BWRX-300 Safety Goals and PSA Objectives

Two PSA levels are applied that estimate the overall risk to the surrounding environment. Each level introduces a specific aspect of overall risk:

- Level 1 estimates the first measure of risk (core damage frequency)
- Level 2 estimates the second measure of risk (radioactivity release)

The two quantitative PSA safety goals are:

- Core Damage Frequency (CDF)
- Large Release Frequency (LRF)

The BWRX plant safety goals for core damage (10^{-6}/yr), and large release frequencies (10^{-7}/yr) are listed in PSR Subchapter 15.3 Table 15.3-3. These are more restrictive than the safety goals typically applied by IAEA member states as documented in IAEA-TECDOC-1874, "Hierarchical Structure of Safety Goals for Nuclear Installations," (Reference 15.6-13), to reflect the advanced nature of the design.

The design phase PSA model discussed in this subchapter represents the standard plant BWRX-300 baseline design. This baseline PSA is subsequently used to develop the site-specific PSA. The objectives of the PSA are listed in Table 15.6- 1: Probabilistic Safety Assessment Objectives.

The BWRX-300 PSA is performed in an iterative manner with the design development used to evaluate and improve the risk aspects of the BWRX-300 design. A key objective of the PSA evaluation is to demonstrate that the BWRX-300 has been designed with highly reliable and available passive safety functions with redundancy and diversity to ensure that all established safety goals are met with margin with a balanced risk profile.

The BWRX-300 design considers guidance and goals for events that are beyond what is typically referred to as the design basis of the plant. For the BWRX-300, Severe Accident (SA) issues are addressed during the design stage to take full advantage of the insights gained from the PSA as well as from operating experience, SA research and accident analysis. The insights are used to identify design features that reduce the likelihood that SAs will occur and to mitigate the consequences of SAs.

FAP item PSR15.6-39 in Appendix B relates to developing numerical on and off-site dose-based targets, individual risk, and societal risk targets.

Probabilistic Safety Assessment Scope

The design stage PSA includes a Level 1 and Level 2 PSA that meets the performance requirements of the American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS) "Standard for Level 1/Large Early Release Frequency Probabilistic Risk." RA-S-1.1-2022, (Reference 15.6-14) and RA-S-1-2024, "Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs)," (Reference 15.6-15). Other important sources of PSA guidance that have been used during the PSA development are IAEA SSG-3, "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plant," (Reference 15.6-16) and IAEA SSG-4, "Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants," (Reference 15.6-17).

The PSA presented reflects the latest full iteration and assessment of the model and therefore aligns with the design at the time of the analysis. Due to the stage in the design development, some aspects of the PSA are more developed than others.

The scope of the PSA covered in this PSR subchapter is:

- Internal events Level 1 PSA at full power and low power and shutdown
- Internal events Level 2 PSA at full power
- Internal fire Level 1 and Level 2 PSA at full power
- Internal flooding Level 1 PSA at full power
- Seismic PSA Level 1 PSA at full power

- High wind Level 1 and Level 2 PSA at full power
- Spent fuel pool PSA
- Fuel and heavy load movements PSA

The BWRX-300 design phase PSA uses current information available from the BWRX-300 plant design and procedures. Periodic updates of the PSA are required after the plant begins operation. Component failure data is based on generic United States industry data considering the BWRX-300 design. This data and the assumptions used to develop the PSA are selected to be as realistic as possible. Based upon the state of the BWRX-300 plant design, when design, site or programmatic information is not available, the PSA models the various elements in a conservative manner (e.g., human error probabilities, maintenance unavailability's, component failure rates, flood and fire initiation, propagation, and their effects).

The FAP in Appendix B includes actions to develop a full scope PSA, including a fully developed Level 1, Level 2 and Level 3 PSA for all internal events and hazards, for all operating modes. This will enable calculation of both on and off-site doses and risk, accounting for all potential radiological releases from the site, which are not part of normal operation.

Methodology

The BWRX-300 PSA is performed in an iterative manner with the BWRX-300 design development to evaluate and improve the risk aspects of the BWRX-300 design.

The design phase PSA for BWRX-300 covers all relevant Initiating Events (IEs). The event types investigated include:

- Internal IEs (internal failures and disturbances)
- Loss of Preferred Power (LOPP) – plant-centred, grid-related, and switchyard-centred
- Internal hazards (e.g., fire, flooding, and lifting of heavy loads)
- External hazards (e.g., adverse weather conditions and seismic events)

For the analysis of external hazard initiating events, possible combinations of external hazards are addressed based on the scope of the individual hazard assessment. For example, high wind, causing loss of the external grid, is considered in the high wind analysis.

The design phase PSA covers both full power and low-power and shutdown operations, including main and supporting systems and components, main operator actions and the relevant event and system dependencies, interconnections, and Common Cause Failure (CCF) relationships.

The development of BWRX-300 PSA models is conducted with the Electric Power Research Institute (EPRI) integrated risk frequency and consequences technology suite of software which include EPRI 3003010659, "FRANX," (Reference 15.6-18) used for fire PSA model development and the EPRI 3003030050, "Phoenix Architect Module," (Reference 15.6-19), which includes the following:

- Computer Aided Fault Tree Analysis (CAFTA) for event tree, fault tree and cutset development and viewing purposes
- Phoenix Application Programming Interface (API) for model integration and one-top development
- PRAQuant for quantification processes, as well as for sensitivity runs

- Human Reliability Analysis (HRA) calculator for Human Error Probabilities (HEPs) and operator action dependency analysis, EPRI 3002010680, “The EPRI Human Reliability Analysis Calculator Software Manual,” (Reference 15.6-20)
- EPRI 3003000578, “Uncertainty Evaluation Tool UNCERT,” for uncertainty analysis (Reference 15.6-21)

The PSA model is integrated and quantified using the computer codes CAFTA, PRAQuant, and Fault Tree Reliability Evaluation Expert (FTREX) (Reference 15.6-22). These computer codes have been demonstrated throughout the industry to produce appropriate results. No method specific limitations have been identified regarding the software tools or the methodology implemented to quantify the model.

Using CAFTA, the BWRX-300 PSA model is developed by merging all model event trees, system fault trees, IEs and associated basic event databases. A top logic fault tree is created using CAFTA. All system fault trees are merged with the top logic fault tree. The fault tree model top gates are quantified to generate cutsets and calculate total core damage and large release frequencies. Individual Event Sequences (ES) are quantified to determine frequencies for the various accident sequence end states and release categories for the Level 2 PSA. Additionally, the linked/merged fault tree is quantified to generate minimal cutsets, which include identifiers to link them to the event tree sequences.

The following areas are addressed in the design phase PSA, whilst a flowchart representation is provided in Figure 15.6- 2:

- BWRX-300 risk results compared to safety goals, including:
  - Core damage frequency
  - Large release frequency
- IE selection, grouping and frequency for each analysed plant operating state
- ES modelling and quantification for accident sequence end state and release category
- System analysis commensurate with design stage
- Success criteria
- Component reliability data (including CCF data and modelling principles)
- Human reliability analysis (including operator action dependency analysis)
- Structural analysis of the containment
- Level 2 containment event tree development
- Release category definition
- Mechanistic source term analysis for each release category
- Uncertainty and sensitivity analysis
- Results analysis – importances and risk insights
- Model documentation

The design phase PSA includes the PSA models as well as documentation. The documentation explains: pertinent plant characteristics, modelling assumptions and techniques, model structure, data values and sources used in the model, and the analysis results. The documentation is explained in a way that makes it possible to review and replicate the analyses.

All work for the design phase PSA is performed in accordance with GEH’s NEDO-11209-A, “Quality Assurance Program Description,” (Reference 15.6-23).

A full scope self-assessment and peer review of all internal and external events models is planned for the PSA model, see FAP item PSR15.6-60 in Appendix B. The planned PSA peer review will assess the technical acceptability of the model and results against relevant PSA standards, such as the ASME/ANS RA-S-1.1-2022 (Reference 15.6-14). The results of the peer review will include any gaps to meeting the standards, limitations arising from the maturity of the design and operational details, as well as plans to address each identified issue.

15.6.1 Level 1 Probabilistic Safety Assessment

The ASME/ANS RA-S-1.1-2022 (Reference 15.6-14) standard presents requirements for a Level 1 PSA while at-power for the evaluation of CDF. The Low Power and Shutdown (LPSD) PSA is developed following the requirements of the standard for LPSD, ASME 58.22-2014, “Requirements for Low Power and Shutdown Probabilistic Risk Assessment,” (Reference 15.6-24), 2017, which is issued for trial use and pilot application. After the trial use, feedback was provided to the PSA Standard Committee and the LPSD standard is being revised.

Figure 15.6- 2 shows the principal steps in the PSA. The BWRX-300 Level 1 internal events analysis includes the following steps which are discussed in turn below:

- Initiating event analysis
- Accident sequence analysis
- Success criteria analysis
- Systems analysis
- Data analysis (including common cause analysis)
- Human reliability analysis
- Model Integration & Quantification
- Uncertainty analysis

The definition of the Plant Operating States (POSs) and the split between the Full Power Internal Events (FPIE) model and the LPSD model is set out in the section below.

15.6.1.1 Plant Operating States

The objective of identifying POSs is to define multiple sets of unique reactor and plant conditions for the purpose of identifying and evaluating the plant response to events which have the potential to lead to core damage and/or large release. Each POS is used to separately evaluate the selection of applicable initiating events, definition of accident sequences, establishment of system success criteria, and for accident sequence quantification. Together the sets of POSs cover the entire spectrum of full power and low power and shutdown operation.

The POS analysis uses a structured process to identify and define a complete set of plant operating states to be analysed in the PSA. The POS analysis determines the POS frequencies and durations and representative decay heat removal associated with each POS. Table 15.6- 2 lists the different operational modes of the BWRX-300 plant.

15.6.1.1.1 Plant Conditions Covered by Full Power Internal Events PSA and Low Power and Shutdown PSA

The first phase division that must be made is between normal full power operation and shutdown operation. The FPIE PSA addresses plant operation and actions required to maintain a safe and stable state for prolonged time. The FPIE PSA assesses events that cause disruption to that operation and result in a plant trip and subsequent response. Necessary response functions are assessed for a mission time of at least 24 hours after the initiating event. It is inherently assumed that failures after this period can be recovered by plant staff and that the plant can be maintained in a safe and stable state. The success end states of the FPIE PSA represent an ending of that analysis and further examination in the LPSD PSA is not required.

In order to transition from Mode 1 to Mode 3, control rods are inserted to lower power. Actual full-power operation ends when control rods are inserted to lower power. During the period between control rod insertion and loss of the main condenser vacuum, the reactor condition is similar to full-power operation with the exception that reactivity is lowered by control rod insertion and the steam is passed to the main condenser through the turbine bypass valve. It is therefore deemed that this period (Mode 2) can be bounded by FPIE PSA with following considerations.

- Decay heat from a low power condition is bounded by that at rated power
- After SCRAM (soft shutdown or manual scram), additional reactivity control is not needed although this is always examined in the FPIE PSA
- During Mode 3 and Mode 4, decay heat is removed by Nuclear Boiler System (NBS)
- Before the SCRAM, containment is de-inerted. If this period is bounded by the FPIE PSA, there is a period where containment is de-inerted in the FPIE PSA. However, since this can be probabilistically addressed in Level 2 PSA, the POS is not divided according to the containment inerting condition.

During startup (Mode 2), the control rods are withdrawn to achieve criticality after pre heat-up using decay heat. It is deemed that the period between control rods withdrawal and start of rated power operation can be bounded by the FPIE PSA with the following considerations.

- Reactivity and decay heat from a low power condition is bounded by that at rated power
- When control rods are withdrawn, containment is still de-inerted. Similar to the power descension process discussed above, there is a period where containment is de-inerted in the FPIE PSA. Since this can be probabilistically addressed in Level 2 PSA, the POS is not divided according to the containment inerting condition.

As a result, LPSD PSA covers the LPSD period between loss of the main condenser vacuum and withdrawal of control rods.

15.6.1.2 Initiating Events Analysis

15.6.1.2.1 Methodology

The first step in developing the design phase PSA is the identification and quantification of the IEs to be used in the sequence analysis. IEs have historically been broadly classified as either “internal” or “external” events. An IE may result from human causes, equipment failure from causes internal to the plant (e.g., hardware faults, floods, or fires) or external to the plant (e.g., earthquakes or high winds), or combinations thereof. The focus of this section is on internal IEs. The Internal IE PSA assesses events that are caused by systems or components located within the site structures. An exception of this is the LOPP which is analysed within the internal events. Internal and external hazard induced IEs (e.g., seismic events, internal floods) are discussed in Section 15.6.2. IEs during shutdown, excluding sabotage, are discussed in Section 15.6.1.8 and spent fuel pool analysis in Section 15.6.1.9.

15.6.1.2.2 Initiating Event Identification

A systematic approach was used to identify events that challenge normal plant operation and require successful mitigation to prevent radionuclide release. IAEA-TECDOC-1804, “Attributes of Full Scope Level 1 Probabilistic Safety Analysis,” (Reference 15.6-25) provides the following IE definition: “an event which could directly lead to core damage or challenges normal plant operation and requires successful mitigation to prevent core damage.”

A comprehensive identification of IEs was conducted, including a review of existing Boiling Water Reactor (BWR) PSAs and generic sources. Generic lists of IEs from EPRI ALWR URD NP-2230 “EPRI-ALWR Utility Requirements Document,” (Reference 15.6-26) and NUREG/CR-5750, “Rates of Initiating Events at U.S. Nuclear Power Plants,” (Reference 15.6-27), were reviewed and compared with the 2015 IE data from NUREG/CR-6928, “Industry-

Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants", (Reference 15.6-28). The IEs identified typically include transients of various types, Loss-of-Coolant Accidents (LOCAs) and support system initiators.

In addition to the identification of generic IEs, a systematic review of BWRX-300 systems using the available Failure Modes and Effects Analysis (FMEAs), system design descriptions, and design workbooks was conducted. The review considered initiating events from multiple failures including equipment failures resulting from common causes within the same system. The existing list of known initiators from the 005N3558 "BWRX-300 Fault Evaluation," (Reference 15.6-29) was also reviewed for consistency.

In addition, planned and unplanned manual shutdowns that seldom place demands on any standby safety equipment are treated as IEs because of their high frequency and because they represent changes in operating states that result in the available equipment demands to reach a safe shutdown condition. Support system failures which would result in a requirement for the plant to be shutdown within a short period of time, for example loss of certain electrical buses, are modelled as a manual trip.

Certain support system failures, which could lead to a plant trip, are modelled with IE fault trees to ensure that all dependencies are appropriately captured. They are developed with guidance found in ERPRI TR-1016741, "Support System Initiating Events, Identification and Quantification Guideline," (Reference 15.6-30) using the 'Explicit Event Approach'. IE fault trees are developed to use run failures as the specific IE, with units of 'failures per year'. In many cases, for the failure to lead to a full failure of the system and plant trip, other events in the IE Fault Tree that could be combined with the yearly failures must be in unitless probabilities. For the non-yearly run failures, a mission time of 24 hours is used since that is a reasonably conservative surrogate for the repair time of the originally failed component. This work was undertaken as part of the systems analysis task.

Human error induced IEs are also considered for these analyses, although the analysis to date has not identified any human actions that would cause an initiating event that would not already be covered by the general transient occurrence data (Type B events).

15.6.1.2.3 Screening of Initiating Events Candidates

The requirements for screening potential IE candidates from the PSA are discussed in IAEA-TECDOC-1804 (Reference 15.6-25) and the ASME/ANS Standard RA-S-1.1-2022 (Reference 15.6-14). Based on these references, the IE candidates identified are excluded from further consideration if they meet one of the following criteria:

- The event does not lead to the IE as defined in the PSA
- The event does not correspond to the scope of the PSA
- The frequency of the event is less than the truncation value related to the accident sequence frequency, and the event does not involve an Interfacing Systems LOCA (ISLOCA), containment bypass, or Reactor Pressure Vessel (RPV) rupture. For these events, the truncation value is at least one order of magnitude lower than the truncation value accepted in the PSA.
- The resulting reactor shutdown during at-power POS is not an immediate occurrence. That is, the event does not require the plant to transfer to shutdown conditions until a defined amount of time has elapsed, the condition is detectable before plant systems are required to respond, and there is a high degree of certainty (based on supporting calculations), that the condition can be detected and corrected before normal plant operation is curtailed (either administratively or automatically).

Based on the above criteria, the IE screening is limited to those events that do not lead to an IE as defined in the PSA, and those events where a shutdown occurs prior to the conditions being corrected with certainty. Screening is carefully and conservatively applied, especially early in design where the impact for an event may not be fully understood without design details fully developed. Screening of internal and external hazards is described separately in later sections in this subchapter.

15.6.1.2.4 Initiating Event Grouping

Individual IEs that require similar response from front-line and auxiliary systems and operators are combined into IE groups. Each IE group is represented by the limiting IE or the hypothetical worst-case IE. After IEs were grouped, the event sequences were compared to ensure the IEs in each group do not have an effect on or dependency with the mitigating systems credited in the corresponding event tree.

15.6.1.2.5 Data Collection for Initiating Events Frequencies

In this step, generic data in the public domain is collected and reviewed for applicability and use for the grouped IEs. The IE data was reviewed for applicability for the BWRX-300. The 2015 update to NUREG/CR-6928 (Reference 15.6-28) contains U.S. data used for most BWR PSAs. The source data includes estimates for a range of events including rare events such as Large Loss of Coolant Accident (LLOCA) and excessive LOCA. NUREG/CR-6928 also includes uncertainty estimates for each IE.

As the BWRX-300 reactor vessel and attached piping are unique with respect to the existing BWR fleet (whose experience comprises the basis for estimated LOCA frequencies), a detailed LOCA evaluation was performed for the BWRX-300 PSA. The current approach is to use generic data scaled for the design-specific pipe configurations and the excessive LOCA frequency is based on available industry generic estimates with consideration given to the unique features of the BWRX-300 design.

Plant-specific IEs, such as those developed using FMEAs are typically estimated using component-based data such as the component data in NUREG/CR-6928 (Reference 15.6-28).

Additional FMEAs and detailed reviews for potential system initiators will be conducted as the design evolves, see FAP item PSR15.6 - 54. When analysing IE frequencies for a specific site, site-specific data collection may be necessary. For example, a site-specific LOPP frequency and LOPP recovery curve will be developed.

15.6.1.2.6 Frequency Quantification

IE frequencies are calculated with units per reactor operating year. A recovery rule is then applied which converts frequencies in units per calendar year. When analysing IEs for LPSD, the IE frequencies are input based on reactor “operating” year. A recovery is then appended that corrects for time in each POS based on a plant availability factor.

15.6.1.2.7 Task Outputs and Preliminary Results

The IEs were derived for internal events at-power and for low power shutdown states.

The summary report, 008N9751 (Reference 15.6-10) includes the complete list of initiating events and frequencies.

15.6.1.3 Accident Sequence Analysis and Success Criteria

15.6.1.3.1 Success Criteria

The BWRX-300 success criteria analysis is integrated with the accident sequence analysis.

The main objective of success criteria formulation is to determine for given IEs what represents a successful or unsuccessful plant response and to translate this information into detailed plant system and operator action success criteria.

Success criteria are defined for the BWRX-300 on several different levels. The highest level of success criteria development is to determine what constitutes mitigation of any IE (i.e., prevention of core damage).

In the BWRX-300 success criteria analysis, core damage is defined as a peak cladding temperature above 982°C.

This is consistent with the core damage definition in ASME/ANS RA-S-1.1-2022 (Reference 15.6-14) stated to be: “uncovery and heat up of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and involving enough of the core, if released, to result in offsite public health effects.”

On a lower level, success criteria are developed to support the Fundamental Safety Functions (FSF) required to mitigate core damage. The success criteria supporting each safety function are the minimum requirements necessary to achieve safe, stable conditions, (i.e., to protect the fuel and prevent release of radionuclides to the environment). Stable conditions are determined by the ability to maintain each safety function for long-term operation. The BWRX-300 Safety Strategy, 006N5064 (Reference 15.6-11) describes three FSFs:

- Reactivity control - to achieve subcriticality and maintain the reactor in a subcritical state (combined with adequate core cooing and/or containment heat removal functions if appropriate) so that core damage and preceding containment failure are avoided.
- Core cooling - adequate core cooling is provided to prevent core damage and the reactor is maintained in a safe-and-stable condition.
- Containment system integrity - ensure that the containment pressure does not exceed the ultimate containment capacity, and containment isolation occurs when required.

Developing the functional success criteria requires an assessment of what front-line systems can provide in terms of mitigating functions and determining their requirement for fulfilling those functions. Examples include determining how many trains of a certain system acceptably perform a function for a given sub-group of IEs. Best-estimate analyses are employed using the EPRI Modular Accident Analysis Program (MAAP) 5.05 software. MAAP is a fast-running computer code that simulates the response of light water and heavy water moderated nuclear power plants for both current and ALWR designs. It can simulate LOCA and non-LOCA transients for PSA applications as well as severe accident sequences. MAAP is not used for modelling of BWRX-300 ATWS sequences. Transient Reactor Analysis Code GEH (TRACG) will be used for success criteria analysis for ATWS events, but this is not yet completed. The plant model and parameters used for thermal-hydraulic analyses are established in a way that provides sufficient resolution and reflects the actual design and operational features of the plant.

Success criteria analysis also utilizes expert judgment to assess the conditions or response of systems, structures, and components in situations when there is a lack of available information, knowledge, or analytical methods upon which a prediction can be based, if it can be demonstrated that the variability and uncertainty potentially inherent in the assessment does not significantly impact on the PSA models and results. The use of expert judgment is discussed in the ASME/ANS RA-S-1.1-2022 (Reference 15.6-14).

Table 15.6- 3 presents the key mitigating systems credited for each of the fundamental safety functions, mapped to the critical safety function criteria used in the MAAP analysis.

Following from the functional success criteria, supporting success criteria are determined. This includes timing calculations for mission times and human actions, inventory availability determination, and any other system or train-level success criteria development.

A mission time to achieve a stable end state after an IE for the accident sequences is determined. As a first approach, a general mission time of 24 hours is assumed for Basic

Events (BEs). A longer mission time of 72 hours is used for accident sequences involving passive systems, such as the Isolation Condenser System (ICS), due to the longer times required to reach a stable state. The available inventories of fuel, water or air in tanks are compared with those required to support each success criterion, for the assumed mission time, and the model reflects the results of this comparison.

More information on the MAAP analysis and resulting success criteria is presented in the summary report, 008N9751 (Reference 15.6-10).

15.6.1.3.2 Accident Sequence Analysis

The role of an event tree is graphical expression of IE groups, success criteria and sequence end points. The basic concept is to prepare an event tree for each IE group defined in each IE analysis task.

The event tree models include the set of safety functions needed to mitigate each IE. The objectives of accident sequence analysis are to ensure that the response of the plant's systems and operators to an IE is reflected in the assessment of risk in such a way that:

- Significant operator actions, mitigation systems, and phenomena that influence or determine the course of sequences are appropriately included in the accident sequence model and sequence definition
- Plant-specific dependencies due to IEs, human interfaces, functional dependencies, environmental, and spatial impact, and CCFs are reflected in the accident sequence structure
- The individual function successes, mission times, and time windows for operator actions for each critical safety function modelled in the accident sequences reflects the success criteria evaluated
- End states are clearly defined to be either core/fuel damage or successful prevention, with the capability to support the interface between Level 1 and Level 2 PSA
- The accident sequences are defined for the selected set of IEs, POSs, and times that a POS can occur

For the BWRX-300, the event trees are generally small event trees developed using the CAFTA software. Event tree headings are largely based on top-level system functions, with functional fault trees added to connect the models to system and train failure events.

The ES analysis meets the ASME PSA Standard ASME/ANS RA-S-1.1-2022 (Reference 15.6-14).

IE groups are studied and organized based on IAEA-TECDOC-1804, (Reference 15.6-25). "For each IE group for internal events, internal hazards, and external hazards for each POS the accident progression for all sequences is identified and justified. For each IE group the accident sequence models are developed. Accident sequence models explicitly address realistic plant behaviour in response to IE in terms of normal plant systems operation, operator actions, and mitigation systems that support the key safety functions necessary to achieve a stable safe state."

Each accident sequence is analysed until one of the defined end states are reached. The end states are either non-successful (e.g., core damage) or a safe stable state, where long-term stability is ensured. For non-risk significant sequences, where specific thermal-hydraulic analysis has not been conducted to support the success criteria development, conservative expert judgement is used supported by knowledge of expected similar Systems, Structures, and Components (SSCs) design or functionality in other reactors (current reactor fleet, etc.)

The accident progression analysis is performed for each sequence until a safe, stable, long-term condition is reached or until core/fuel damage occurs, to determine if there is a cliff-edge effect beyond the mission time used in the PSA. The safe stable state for each end state is defined to ensure:

- The core remains subcritical over the duration of the event
- Equilibrium conditions are obtained, and the conditions are trending in a safe direction
- Inventories are not lost within the defined mission time, or within a short time frame beyond the defined mission time
- Containment cooling is provided, with temperatures stabilized to the level where the heat removal rate and the decay heat are balanced

ATWS sequences are not grouped into a single event tree. Rather, each IE group has a sequence with SCRAM failure with a transfer to a unique ATWS tree. Those ATWS sequences go either to the general transient ATWS tree, to the LOPP ATWS tree, or are assumed to result in core damage.

Each key safety function's dependence on the success or failure of preceding functions and the impact on accident progression are addressed. This is called a functional dependency that affects the availability of subsequent mitigation features.

Fault trees are developed in a way as to capture all dependencies. For example, impact from a loss of electrical bus IE (dependency between the bus and mitigating function), is captured in the mitigating function fault trees. When accident progression and associated success criteria notably change after failure of specific functions, a linked event tree(s) is prepared, such as consequential LOPP link trees for transients with consequential LOPP.

Dependencies between event trees are inherently preserved by the underlying system fault trees that share common BEs and account for equipment that has already failed.

15.6.1.3.3 End States of Event Sequences

The event trees identify the potential sequences that can lead to radionuclide release. Many of the sequences have common characteristics with respect to the challenge on the containment radionuclide barrier. These sequences are grouped into core damage classes that are analysed in the Level 2 PSA. The end states of the ESs developed for the BWRX-300 PSA are defined to facilitate containment performance analysis and provide the link between core damage and a release category.

The core damage sequences are grouped together based upon the overall challenge to the containment barrier and defined as:

- OK: The core is successfully cooled, and the containment is intact. There is no core damage in these events.
- CD I: The containment is intact when core damage occurs and the RPV is at low (or controlled) pressure.
- CD II: The containment is breached, either due to over pressurisation or venting, while the core is successfully cooled. Core damage results due to failure of long-term heat removal to maintain core cooling.
- CD III: The containment is intact when core damage occurs and there is high RPV pressure at the time of RPV failure.
- CD IV: Core damage results from an accident sequence with an initial failure of effective reactivity control (e.g., ATWS due to failure of Reactor Protection System (RPS), control rod binding). This has the potential to affect the containment in a more

severe manner than the CD I and CD III because more energy is deposited into the containment prior to RPV failure. All CD IV end states could be treated as CD I or CD III (depending on the RPV pressure) without affecting the results of the containment analysis. This end state has been retained to more easily allow for sensitivity analyses related to reactivity control.

- CD V: The containment is bypassed at the time of core damage.
- CD VR: Core damage occurs due to RPV ruptures in the lower or mid-vessel regions.

15.6.1.3.4 Task Outputs

Event trees were developed for the following events. All IEs identified are considered in one of these event trees:

- T-GEN (general transient)
- T-PCS (loss of condenser heat sink)
- T-LOPP (loss-of-preferred power)
- Break Outside Containment (BOC)-MSL (main steam line break outside containment)
- BOC-FDWA (feedwater line break outside containment)
- ELOCA (excessive loss of coolant accident)
- LLOCA (large loss of coolant accident)
- MLOCA (Medium Loss of Coolant Accident)
- SLOCA (small loss of coolant accident)
- MAN-SD (manual shutdown)
- AT-T-LOPP (a transfer event tree from T-LOPP event sequences with reactivity control failures)
- AT-T-GEN (a transfer event tree from T-GEN events sequences with reactivity control failures)

15.6.1.4 System Analysis

The system analysis is performed for each plant system represented in the IE and accident sequence for each POS in such a way that:

- All safety functions modelled in accident sequence or system models meet the derived success criteria
- System-level success criteria, mission times, time windows for operator actions, different initial system alignments and assumptions provide the basis for the system logic models reflected in the model. A reasonably complete set of system failure and unavailability modes for each system is represented
- Human errors and operator actions that influence the system unavailability or the system contribution to accident sequences are identified for development as part of the HRA element
- Intra-system dependencies and inter-system dependencies including functional, human, phenomenological, and CCFs that influence system unavailability or the system contribution to accident sequence frequencies are identified

Other objectives include:

- Considering credible failure modes

- Modelling each failure mode impact on system performance
- Including support system failure modes in the front-line system fault trees
- Creating linked fault tree models that can be solved efficiently
- Creating fault tree models where solutions (i.e., cutsets) are easily understood

The system analysis builds logic for each function identified within a system top event. The top event links with the sequence logic, or with other system logic.

15.6.1.4.1 Systems Credited in the Probabilistic Safety Assessment

The following systems are modelled in the PSA:

- Safety Class 1/2/3 Distributed Control and Information System (DCIS)

  The reference PSA models Defence Line 2 (DL2), Defence Line 3 (DL 3), and Defence Line 4a (DL4a) I&C functions. The common cause software failure is modelled for DL 3 and DL 2 I&C systems. Each CCF is conservatively assumed to fail all functions of the associated software platform. DL4a I&C system is implemented in an analogue hardware platform. The design of the I&C has significantly changed since the reference model was completed and work is underway to update the I&C modelling to align with the design, using a methodology based on the EPRI 2024 White Paper EPRI 3002029332, “Untangling Systematic Failures, Dependencies, and Common Cause Failures in Digital Systems: Leveraging EPRI’s Digital Engineering Framework for Probabilistic Risk Assessment (PRA) Modelling”. This is captured by FAP item PSR15.6 – 59 in Appendix B.

- Isolation Condenser System

  The ICS’s function is to remove decay heat from the reactor by condensing steam in the ICS heat exchangers.

- Reactor Isolation Function

  The reactor isolation function mitigates the effects of large and medium sized pipe break LOCAs. The term “RPV isolation system,” is used to refer to reactor isolation valve closure. The system model is a surrogate for valves that are part of the NBS.

- Control Rod Insertion Function

  The Control Rod Drive (CRD) system performs several insertion functions and consists of these design features: Fine Motion Control Rod Drive (FMCRDs), Hydraulic Control Units (HCUs), and the CRD hydraulic subsystem.

  The PSA-credited function of the control rod insertion is to insert negative reactivity into the reactor core rapidly upon a scram signal. Subcriticality is achieved with the negative reactivity insertion and terminates fission heat generation.

  The CRD system also provides an RPV inventory makeup function.

- Feedwater (FW) Runback System

  The FW runback system provides negative reactivity in an ATWS condition by reducing FW flow resulting in increased core voiding (the BWRX-300 has a negative reactivity void coefficient).

- The FW runback system is part of the anticipatory trip system, which provides a signal to the operating FW pump to reduce the flow to the reactor. It is part of DL 2 and is designed to insert negative reactivity in the event of a condition that could result in a scram signal.

- Containment Isolation Function

  The containment isolation function provides isolation of the containment in the event of accidents or other conditions and prevents unfiltered radioactive releases before they exceed allowable limits.

  The containment isolation system uses sensors that interface with the I&C and electrical penetrations required to route signals in and out of containment. This system is designed to automatically isolate the containment and prevent the release of radioactive contaminants into the environment in the event of a condition that could result in core damage. This is modelled in the Level 2 PSA.

- Boron Injection System

  The Boron Injection System (BIS) provides a separate, diverse means, defence-in-depth backup system to the CRD system for manually inserting negative reactivity into the reactor core for beyond design basis accidents. All equipment is located outside primary containment to allow easy access for testing and inspection activities during all plant operating conditions.

  The BIS utilizes an aqueous solution of highly enriched sodium pentaborate decahydrate for reactivity control. The sodium pentaborate solution temperature is maintained above the solubility temperature by the placement of the system within the Reactor Building (RB).

- CRD Injection Function

  The BWRX-300 CRD System consists of the FMCRDs, the HCUs, and the CRD Hydraulic system. The focus of this system for PSA is the CRD hydraulic subsystem that is used for inventory makeup and flow to the Shutdown Cooling (SDC) pumps.

  The CRD hydraulic subsystem provides clean, demineralised water that is regulated and distributed to provide charging to the scram accumulators and purge water flow to the FMCRDs during normal operation. The CRD hydraulic subsystem is also the source of purging water to the SDC system pumps and the NBS reactor water level reference leg instrument lines. Additionally, the CRD hydraulic subsystem provides high pressure injection to the reactor. This makeup water is supplied to the reactor via the drives.

- Power Conversion Function

  The Power Conversion System (PCS), as modelled in the PSA, removes decay heat from the reactor by providing a pathway for FW from the condenser to the reactor and for steam from the reactor back to the condenser. Because the PSA model assumes a scram has occurred or is warranted, the full power function of providing steam to the turbine for power generation is not considered.

  There is only one function for the power conversion function modelled in the PSA. This function is providing water from the condenser, via the condensate pumps, FW heaters and FW pumps, to the reactor where it is heated, and steam is produced. Steam is transferred to the condenser via the turbine bypass valves.

- Cooling Water Systems

  The Plant Cooling Water system (PCW) removes heat from loads in both the RB and Turbine Building (TB), dividing PCW loads into two subsystems: reactor component cooling water subsystem and turbine component cooling water subsystem.

  PCW is a closed cooling water system supported by cooling from a portion of the circulating water system.

- DC Power

  The electrical distribution system is an integrated power supply and distribution system for the power plant. Three plant systems constitute the overall electrical system: R10 - Safety Class 1 Electrical Distribution System, R20 - Safety Class 2 and 3 Electrical Distribution System, and the R30 - Non-Safety Electrical Distribution System. The three plant systems are grouped based on safety classification with R10 being Safety Class 1 functions, R20 being Safety Class 2 and Safety Class 3 functions, and R30 being non-safety functions.

  The electrical system powers automatic shutdown and decay heat removal functions. The Safety Class 1 portion of the electrical distribution system (includes DC) is limited to supplying power to Safety Class 1 SSCs within the RB rooms.

  Safety Class 1 DC power three division (A, B, and C) arrangement supplies DC power to various loads. Each division has a DC battery and two redundant battery chargers powered from the Safety Class 2 and 3 Electrical Distribution System AC power system.

  The primary load of the Safety Class 1 Electrical Distribution system is the DCIS.

- AC Power

  AC power modelled in the PSA, is providing medium and low voltage AC power to plant components. The following AC buses are modelled:

  - Buses A1 and B1 provide 4160V AC power to Balance of Plant (BOP) components such as FW pumps and condensate pumps. These buses are not backed by diesel generator.
  - Buses A2 and B2 provide 4160V AC power to other components, such as control rod drive pumps and reactor component cooling pumps. These buses are each backed by a standby diesel generator in the event of LOPP.
  - Divisions 1, 2 and 3 provide 480V AC power to Motor Control Centre (MCCs), Motor Operated Valves (MOVs), smaller motors, and other plant equipment.
  - Corium Shield
  - The corium shield prevents core melt from damaging the containment liner once the core has broken through the bottom of the RPV. The system is still in design and may not reflect the final system.
  - The corium shield is a risk reduction design feature that includes a refractory material below the RPV. After core damage, in cases where the RPV is assumed to be at a low enough pressure to preclude direct containment heating, the core debris eventually migrates from the core region to the RPV lower head and exits the through a breach (e.g., lower head failure or CRD housing failure). The refractory material below the RPV prevents molten core-concrete interaction and any potential ablation of the basemat and accompanying flammable gas generation. This is modelled in the Level 2 PSA.

- Passive Containment Cooling System

  The Passive Containment Cooling System (PCCS) rejects heat into the reactor cavity and/or equipment pool above containment. Supply and discharge connections from the pool are connected to closed loop piping within containment. Heat transfer occurs from the containment to the PCCS by natural convection and condensation. This is modelled in the Level 2 PSA.

- Ultimate Pressure Regulation Function

The Ultimate Pressure Regulation (UPR) function of the RPV provides emergency pressure relief in the event of a severe pressure transient. The design has not been finalised but will likely be provided by a power operated relief valve and rupture disk to be included on each of the ICS steam supply lines. UPR relieves RPV pressure to the containment.

- Containment Filtered Venting

  The containment pressure relief system vents pressure in the containment because of LOCAs, RPV pressure relief, or core melt. By providing a vent to the containment, pressure and temperatures can be maintained. The release is filtered to reduce the amount of fission products. Components such as duct work and filters that are the normal path of containment do not have the ability to vent the pressures seen during an accident. Venting is assumed to be required when no other containment heat removal method succeeds and in certain special situations in which there is an excessive containment pressure load beyond the capacity of PCCS. The system comprises a rupture disk, manual bypass, and an air operated isolation valve. Currently, the design has the effluent go to a pool of water to help limit radiological release.

- Heating Ventilation and Cooling System

  The Heating, Ventilation, and Cooling System (HVS) system provides normal room atmospheric temperature and ventilation control and room cooling during accident scenarios for locations determined to require such cooling.

  Systems assumed to require HVS for successful operation have placeholder transfer gates with an assumed failure point-estimate screening value used in PSA model quantifications. This system will be further developed as design information becomes available, see FAP item PSR15.6 – 58 in Appendix B.

- Plant Pneumatic System

  The plant pneumatic system function provides motive and control air to various plant components. The pneumatic system supports multiple systems and valves. The Plant Pneumatic System consists of two compressor trains, each one able to supply 100% of the plant compressed air requirements.

15.6.1.4.2 Methodology

The BWRX-300 system analysis includes systems modelled in the BWRX-300 PSA, which correspond to the functional headings described in the ESs plus any support systems needed to accomplish those functions. The system modelling methodology was based on guidance taken from: NUREG/CR-2300 “PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants,” (Reference 15.6-31), NUREG/CR-4550 “Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events Appendices,” (Reference 15.6-32), and NUREG/CR-4551 “Evaluation of Severe Accident Risks: Methodology for the Containment, Source Term, Consequence, and Risk Integration Analyses,” (Reference 15.6-33) series. Additional guidance on fault tree modelling, current information for the system studies, and latest results were taken from NUREG-0492 “Fault Tree Handbook,” (Reference 15.6-34) and the “Overview of the PSA Process and Basic PSA Techniques,” (Reference 15.6-35).

A systematic approach is used to identify the systems and functions credited in the BWRX-300 PSA including the frontline systems and support systems. This begins with the accident sequence top event identification, documented in the accident sequence evaluation. Fault trees are then developed for functions credited in the accident sequence modelling based on the documented system-level success criteria for those functions. Several sources of information are considered in the development of the system fault trees including:

- System design documents
- System drawings such as piping & instrumentation diagrams, simplified drawings, and process flow diagrams
- Higher-level architecture documents (e.g., electrical architecture report)
- Technical specifications
- Discussions with system engineers
- Expert judgment

For each system described above, an individual system notebook is created to fully describe the process of developing the associated fault trees, noting that I&C is incorporated into the supported system notebooks as required. Each system notebook discusses the following topics:

- System description, spatial information, and function
- System requirements from the system design description
- Modelled top events and success criteria
- Inputs, requirements, and assumptions
- System model development:
    - System engineer discussions
    - System and component boundaries
    - System alignments
    - Component failure data
    - Common cause failure
    - Human failure events
    - Technical specifications and operating limits
    - Test and maintenance events
    - Support system dependencies
    - Initiating event impact on the system
    - Other modelling details
- Results of system analysis
- Uncertainty analysis
- Open items and risks
- Supporting files

For systems which operate in several different modes or plant operating states, each mode and the functions performed are explained. Only those functions that contribute to plant risk defined by the accident sequences are included. The interfaces and system connections of the system with other systems are described. This also includes the support systems and relevant system components required for the operation of the system. Any other relevant aspects of the system operation including system trips, interlocks and procedural restrictions during accident conditions are also addressed.

Necessary operator actions are identified for systems where manual initiation is necessary or manual backup is credited in the PSA. The post-initiator human failure events (Type C) are identified as part of the success criteria development and system analysis, using operational procedures where available. Significant pre-initiator human failure events (Type A) are identified by considering test and maintenance related to the SSCs modelled in fault trees and are also identified as part of the system analysis.

Systems models are developed that include all component failure modes and unavailability factors that lead to failing to achieve the system function defined by the system success criteria. Component failures that would be beneficial to system operation are not included in the model. System modelling includes the modelling of components shared between systems. An important aspect in ensuring dependencies are accounted for in the model is the consistent naming of BEs in each system model. Likewise, systematic identification and inclusion of inter and intra system CCFs is important to ensure all failure mechanisms resulting in failure to meeting the success criteria have been appropriately captured. It is noted that currently the digital I&C systems are modelled with software CCFs for each DL I&C system.

Uncertainty is categorized into two general sources: data uncertainty and modelling uncertainty. Data uncertainty is evaluated quantitatively using uncertainty associated with the parameter distributions for component unreliability, initiating event frequency, train unavailability, and human error probability. Data uncertainty is evaluated for the final model using sampling techniques (e.g., Monte Carlo) on parametric distributions in the reliability database. The system evaluations in the system notebooks highlight sources of modelling uncertainty which could be significant enough to impact PSA results.

15.6.1.4.3 Fault Trees

One fault tree for each system function is included in the PSA model. If multiple trains perform the function, then each train is modelled. All the logic for a particular system is contained in a single fault tree file.

The fault trees are constructed using the gate and basic event naming conventions. A tree database is stored in the CAFTA database file format.

15.6.1.4.4 Task Outputs and Preliminary Results

The following are key task outputs:

- System notebook for all modelled systems
- System fault trees
- System availability and component failure mode data requirements (interface with data analysis)
- Identification of human actions (interface with human reliability analysis)
- Record of assumptions for each system model

The documentation of the system analysis is constructed to facilitate licensing of the BWRX300 design. It describes the processes used for modelling and quantification. It also includes the generic modelling assumptions. It is constructed with consideration of future updates to the BWRX-300 PSA and for risk-informed applications involving the BWRX-300.

15.6.1.5 Data Analysis

The data analysis provides estimates of the reliability parameters for the reliability models specified under the systems analysis. The reliability models are used in determining the Basic Event (BE) probabilities of specific equipment failures and unavailability factors.

Data analysis is used in deriving the parameter values that estimate system failure probabilities and accident sequence frequencies. These BEs used in the PSA model are outputs from the IE analysis, accident sequence modelling, and system fault tree modelling discussed previously. The PSA BEs include the IE frequencies, component unavailability, component/train unavailability factors (resulting from testing or maintenance), CCF events, and other types of events. At this stage in the design process, there is no plant-specific reliability data available other than that provided by operating experience at existing BWR plants. Therefore, generic data from the nuclear industry and associated uncertainty data is used.

In the absence of actual operating experience for the passive plants, EPRI TR-016780-V3R8, "Advanced Light Water Reactor Utility Requirements Document, (URD) Volume 3, Revision 8: ALWR Passive Plant," (Reference 15.6-36) recommends using failure data for components that are most similar to those used in passive plants. Additional adjustments to the generic data are introduced after analysing the test and maintenance intervals and the environmental factors. Due to the limited operating experience and the lack of plant-specific data, the development of failure rates for equipment reflects appropriate characterisations of the associated uncertainties. The data and basis for test and maintenance unavailabilities are based on bounding generic values and Operational Limits and Conditions allowed outage times. The values will be updated as more information becomes available regarding test and maintenance activities, see FAP item PSR15.6 – 50 in Appendix B.

The level of redundancy in passive plant design and few critical support systems leads to increased focus on CCFs. CCFs are modelled for the components of the same type and size in the same operating and maintenance environment. The CCF alpha factor data from the U.S. Nuclear Regulatory Commission (USNRC) CCF database, "CCF Parameter Estimations, 2020 Update," (Reference 15.6-37) is used in this analysis. Generic CCF factors are used when component-specific data are not available.

15.6.1.5.1 Methodology

In the absence of actual operating experience for the passive plants, generic reliability data from the 2020 update (Reference 15.6-38) to NUREG/CR-6928 is used. Where NUREG/CR-6928 does not provide sufficient detail, the following hierarchy of additional sources is used when required (noting there is no significant overlap in scope of the final three sources):

- NEDE-22056 Revision 2, "Failure Rate Data Manual for GE BWR Components," (Reference 15.6-39)
- INEEL-EXT-98-00892, "Selected Component Failure Rate Values from Fusion Safety Assessment Tasks," (Reference 15.6-40)
- NUREG/CR-5500 Volume 3, "Reliability Study: General Electric Reactor Protection System 1984-1995," (Reference 15.6-41)
- NUREG/IA-0463, "(Availability of) An International Report on Safety Critical Software for Nuclear Reactors by the Regulator Task Force on Safety Critical Software (TF-SCS)," (Reference 15.6-42)

Components are grouped into population groups for parameter estimation. The rationale for grouping components into a homogeneous population for parameter estimation considers the design, environmental, functional, and operational conditions of the components in the as-built and as-operated plant. For parameter estimation, components are grouped according to type and to the detailed usage characteristics. Component boundaries are adopted from the data source used to develop the failure rate data for the components of interest. Appendix B of the PSA Methodology 006N2915 (Reference 15.6-9) provides description and pictorial representation for many of the commonly used components in the PSA.

The component type and failure mode are combined to form the ‘Type Code’. Type codes are component-failure mode pairs that are used to represent a failure probability or failure rate. The type codes are used across several BEs, potentially, to perform BE probability calculations. Type codes are not only associated with a mean failure probability, but also an uncertainty characterisation. This is instantiated as an uncertainty distribution type and uncertainty parameter. There are several BE failure probability calculations used in the BWRX-300 PSA model. The parameters for the calculations are input into the CAFTA database where the probabilities are automatically calculated.

Common Cause Failure Analysis

Dependent events challenge redundancy or diversity and ultimately increase the unavailability of a system. The general approach described in NUREG/CR-6268, INL/EXT-07-12969, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding,” (Reference 15.6-43) is used in the CCF analysis.

The alpha-factor method is used to quantify CCFs in the PSA. A detailed description of the alpha-factor method and its advantages over the older beta-factor and multiple Greek letter methods for modelling CCFs is provided in the report on Guidelines on Modelling CCFs in ASME/ANS RA-S-1.1-2022 (Reference 15.6-14). The alpha-factor method is preferred as it enables better modelling of higher common cause component groups and more accurate modelling of uncertainty in the CCF parameters.

Industry-average estimates for alpha parameters were obtained from the USNRC CCF Parameter Estimations 2020 (Reference 15.6-37). The USNRC CCF database is based on the large amount of nuclear industry operating experience collected in the US, including BWRs. The database is also regularly updated and reflects recent nuclear industry operating experience. If a CCF parameter is defined on a system-by-system basis in the reference, an appropriate parameter is selected on a system-by-system basis. A general parameter (i.e., "Generic CCF distribution" in the reference) is used if no CCF parameter is defined for a component.

CCF alpha factors are identified on a component by component, and system by system basis. The distributions (beta distributions with associated α and β parameters) for each of the alpha factors are presented in the reference and used in the PSA model.

Once the CCF BEs are identified the model utilises the CCF tool in CAFTA to automatically identify all the CCF combinations for a given CCF group and place the appropriate CCF BEs into the fault trees. CAFTA is also used to automatically quantify each of the CCF BEs. As recommended by the CAFTA developers, common cause groups containing more than four components are treated simplistically. CCF events are developed for all combinations of one, two, and three components within the group, with all remaining failure probability assigned to a CCF event of all components failing. This is a conservative representation of the event modelling all components failing, since the CCF probability of all components is overstated, but greatly simplifies the fault tree modelling.

When this treatment is too conservative, the calculations are completed outside of CAFTA and entered manually. In these cases, the CCF combinations are manually input to the fault trees using the parameters for the actual CCF group size and the CCF equations are directly input into the database file.

There are some CCFs for which the CCF tool cannot be used. In these cases, there is no specific data available and engineering judgment or other data sources are used to calculate the CCF events.

15.6.1.5.2 Task Outputs and Preliminary Results

The output of the data analysis task is the BWRX-300 reliability database that supports development of system analysis, human reliability analysis and quantification tasks.

The risk insights of common cause failure analysis at the systems and the plant-level clarify the balance between the design and the reliability of SSCs. Furthermore, these insights help in the implementation of procedures and training to manage the balance between design configuration control and component reliability control.

Documentation requirements are prescribed in IAEA-TECDOC-1804 (Reference 15.6-25). For the data analysis the following tasks are completed:

- The basis of boundaries and rationale behind grouping of components are defined
- The model used to evaluate each basic event probability
- Sources for generic parameter estimates
- Assumptions made in the interpretation of data and the reasoning (based on engineering judgment, systems modelling, operations, and statistical knowledge) supporting its use in parameter estimation
- The basis for the estimates of common cause failure probabilities
- Parameter estimates including the characterisation of uncertainty as appropriate
- The rationale for using generic parameter estimates for multiple POSs
- The derivation of the parameter values is documented
- The information/database is documented and stored in a way which allows reproduction of the data analysis task for example for reliability parameter updates
- The sources of model uncertainty and related assumptions associated with the data analysis are documented
- For CCF analysis:
  - Identification and definition of CCF methods
  - Formulas for CCF basic event calculation
  - Discussion of special CCF type codes and their derivation
  - CCF data

15.6.1.6 Human Reliability Analysis

PSR Subchapter 15.4 covers HRA in more detail. A brief overview is given here.

The HRA process utilises resources from the EPRI suite of HRA tools. The general HRA process follows the following steps:

- Identification of human-interactions
- Capturing key assumptions
- Focusing on the key interactions through screening
- Describing the human actions in detail

- Incorporating performance influencing factors
- Quantifying the HEPs

Three types of human action are addressed:

- Pre-initiating event human actions (known as Type A human actions). Errors or rule violations associated with these actions may result in loss or unavailability of a safety function within a line of protection.
- Human actions involved in the development of an initiating event or plant transient (known as Type B human actions).
- Post-fault human actions (known as Type C human actions). These human actions are required in response to an initiating event as part of a protective measure. For these actions, error could result in failure to control or mitigate the progression of a fault condition.

The human actions, along with the basis, context, and summary of substantiating evidence, are documented in the Human Safety and Reliability Claim database for tracking and future substantiation.

For the Type A human actions, the EPRI HRA Calculator (Reference 15.6-20) is used to derive a HEP based on the Accident Sequence Evaluation Program (ASEP) method. Very few credible Type A actions have been identified. Traditional miscalibration actions have been screened out on the basis that the C36 Technical Specification Monitor A and B (TSM) would detect any such event and alert the operator before the error could lead to an initiating event.

The Type C human actions are modelled as being composed of two elements, a cognitive element, and an execution/action element. The EPRI HRA Calculator uses the cause-based decision tree method and/or the human cognitive reliability/operator reactor experiments to derive a HEP for the cognitive element and the Technique for Human Error Rate Prediction to derive the HEP for the execution/action element.

As the development of the PSA models are in their early stages, screening HEPs are currently used. The EPRI HRA Calculator approach described above has been used to derive screening HEPs for important human actions when at-power. For the low power and shutdown events and spent fuel pool events PSAs, the screening HEPs have been based on engineering judgment, with suitable justification being provided.

The quantification of any HEPs associated with Type B Human Failure Events (HFEs) will be undertaken on a case-by-case basis, using HRA Calculator to apply the most appropriate human error quantification technique for the error being quantified. No Type B HFE have been identified at this time that are not already covered by existing initiating events. Given generic frequency data is used based on industry OPEX, the contribution from human error is already accounted for in the initiating event frequencies.

The HRA Calculator is also used for operator action dependency analysis.

15.6.1.7 Event Sequence Frequency Quantification

The BWRX-300 PSA model consists of event trees and fault trees that are quantified using a fault tree linking process.

The calculation of core/fuel damage and release category frequencies is performed as a single top gate for each sequence and release category. The top gates include all sequences but use a sequence marker to identify the event tree sequences in the Minimal Cutsets (MCS) generated by the single top. The use of a sequence marker results in retaining all the MCSs for that specific sequence but prevents subsuming of non-minimal cutsets among sequences.

The contribution to risk from these non-minimal sequences is generally small, although this can affect the results for specific hazards, such as earthquakes. The sequence logic is also set up to exclude any combinations associated with the success branches in the specific sequence. The individual sequence results can then be combined as necessary for reporting, analysing, or to be used as input for the Level 2 or Level 3 portions of the PSA.

15.6.1.7.1 Methodology

The purpose of the ES frequency quantification is to obtain the Boolean equation corresponding to the radionuclide release. The quantification is developed in terms of MCSs representing the minimal combinations of events that result in radionuclide release.

The following key aspects characterise the release category frequency quantification process:

- Event trees model plant response to each group of IEs
- Fault trees model the behaviour of front-line and support systems
- Integration of event tree and fault tree structures into a single linked model
- Quantification of the linked Boolean model with the probabilistic database and boundary condition files (flag files)

Use of CAFTA for Solving the Probabilistic Safety Assessment

For the Level 1 BWRX-300 PSA model development and quantification, the EPRI Integrated Risk Technology suite of software packaged under the Phoenix Architect is used that includes the following:

- CAFTA for event tree, fault tree and cutset development and viewing purposes
- Phoenix API for model integration and one-top development
- PRAQuant for quantification processes, as well as for sensitivity runs
- FTREX as the quantification engine (cut set generation)

EPRI Integrated Risk Technologies User Group offers the suite of risk software tools (formerly known as a Risk and Reliability Workstation), which have been used for the Level 1 PSA model development and quantification. These risk software tools include CAFTA for event tree and fault tree construction and PRAQUANT for master model integration and quantification. Accident sequence frequencies are derived from the quantification results of a single top master fault tree by post-processing using the sequence markers. The PSA code FTREX is the PSA model quantification engine.

CAFTA has worldwide users at more than 70 power plants and has a very large active user community ranging from power generation to communications, transportation, aviation, and space applications.

The FTREX (Reference 15.6-22) code is used in generating MCSs from fault tree logic models. FTREX uses a zero-suppressed binary decision diagram method for interpreting large fault tree models when developing MCSs. FTREX is built for PSA applications and is applicable to the BWRX-300 PSA without specific limitations.

PSR Chapter 3, Appendix I discusses the computer programs used in the PSA.

Quantification File Structure

The following files are generally associated with the PSA integration and quantification of the Level 1 internal events PSA. Other files may be developed for hazard quantification:

- Event tree files: These files contain the event tree structures for each group of IEs. The radionuclide release sequences of these models are converted into fault tree logic and integrated into the master fault tree file along with the system fault tree logic.
- Fault tree files: A single fault tree file contains all the release sequences, with all the front-line and support systems linked. Each sequence subtree includes a top gate that combines the IE and the functional failures and successes of the sequence.
- Database file: The database contains the inputs, assumptions, probabilities, and frequencies of each of the events associated with the fault tree.
- Quantification file: This file contains the factors and conditions for quantifying the different ESs.
- "Flag" files: "Flag" files contain boundary conditions (e.g., type of IE, assumed plant configuration) used in the quantification of the ESs.
- Recovery files: files are used for post processing of cutsets.

The reliability databases supporting the BWRX-300 PSA include the IE frequencies, component failure frequencies and probabilities, CCF data, component repair times, test intervals and durations, mission times, maintenance unavailability, unavailability due to testing, and human error data. Uncertainties for data values are also included. All the data sources were justified and documented as part of the data analysis task.

Additional Quantification Steps

The quantification process used for the PSA is iterative and includes numerous stages where internal and external review is performed before final results are documented. Key steps performed during the quantification include the following:

- Circular logic: It is possible to generate a master fault tree that has circular logic. This is where a gate is used as input to a second gate that happens to also be an input somewhere in the tree of the first gate. The "Find Circular Logic" tool within CAFTA is used to identify any instances of circular logic. Breaking the logic involves revision to a system fault tree.
- BE consistency check: The IE frequencies and the probabilities associated with BEs of the model should be consistent with the definitions of the events in the context of the logic model. As the PSA cutsets are reviewed, they are reviewed for consistency in terms of the applied assumptions, specific design, and operational experience. A simple example is to verify the assumed time windows for BEs within a cutset match the resulting cutset time window.
- Mutually exclusive event review: The model is solved with and without the mutually exclusive event file to verify the event combinations are removed.
- Human error dependencies: The HRA Calculator is used to perform the HRA dependency analysis. One example of how human failure event dependencies is determined is summarised as follows: All post-initiator human failure event probabilities are set to one or a high value, the single top quantification is performed again, and the most critical human failure event dependencies are apparent in the cutset results. The PSA then uses the results generated in the cutsets to generate recovery rules that change the probability of these joint failures to a value that better

reflects the dependency between these human failure events, taken from the human reliability analysis.

- Truncation justification: To justify that an appropriate truncation value is used, a test for CDF convergence is performed. To test for convergence, the CDF models are solved again with the truncation lowered by an order of magnitude (e.g., if the truncation was set to 10-11, lower this value to 10-12). If resulting CDF increases by more than 5%, the model has not converged. This process is repeated until the CDF increase for an extra decade of truncation is less than 5%. Additionally, to ensure the ASME/ANS RA-S-1.1-2022 (Reference 15.6-14) is met, the last two convergence runs are used to develop a list of risk-significant accident sequences (e.g., contributing greater than 1%) to ensure no new significant accident sequences are identified by lowering the truncation limit further. Following this approach, the cutsets have been generated with a truncation limit of 10-15.
- Importance analysis: This analysis documents the overall contribution of BEs to each phase of the PSA including the Level 1, and Level 2 PSA. Separate importance results are provided for BE types such as IEs, human errors, event class, and release categories. Importance measures are tabulated separately for internal events, internal hazards, and external hazards, and then again for the combined results given the combined (merged) results are developed.
- Uncertainty and sensitivity: Uncertainty analysis to assess statistical and state of knowledge uncertainties. Sensitivity analysis to determine what parameters have an impact on the results.
- Review of the results: ASME/ANS RA-S-1.1-2022 (Reference 15.6-14) and the IAEA-TECDOC-1804 (Reference 15.6-25) require the review of the results in detail to ensure the results are consistent and justified. The steps include review of both risk-significant and non-risk-significant cutsets by knowledgeable staff, and comparison of the results with similar plants. For the BWRX-300, the comparison of the results with similar plants is not possible, other than a general comparison with other BWRs using similar components (e.g., ICS).
- Documentation: This step is key to the use of the PSA for risk-informed applications including licensing. All of the steps discussed above, including the modelling integration and quantification process, are documented in a manner that facilitates external review as well as future upgrades and applications. This includes the clear documentation of assumptions.

15.6.1.7.2 Task Outputs and Preliminary Results

Integration and quantification of the internal events at-power BWRX-300 PSA model results in the following key outputs:

- The final internal events At-power BWRX-300 PSA model files:
  - Single top sequence logic file
  - Single top main fault tree
  - Final merged reliability database
  - Main configuration flag file
  - Recovery rule file
- Core/fuel damage and release category frequencies

- Core/fuel damage and release category frequencies as a function of:
  - Internal events
  - ESs
  - Event class
- Importance characterisation of individual events, in terms of industry standard risk importance measures (e.g., Fussel-Vesely; Risk Achievement Worth (RAW)) relative to the core damage and release category frequency.
- Documentation of the quantification process, including model files, software versions and quantification setup. The results analysis discusses the key initiating event contributions to CDF, top sequence contributions and system, component and HFE importances. The key risk insights are captured and used to develop requirements to feed back into the design development process, as described in the "BWRX PSA Strategy document", NEDC-34158P (Reference 15.6-44). Uncertainty and sensitivity analysis is conducted under a separate task.

Results are presented in PSR Subchapter 15.9 Table 15.9-9 and discussed in Section 15.6.6 and risk insights in Section 15.6.8.

15.6.1.8 Low Power and Shutdown Risks Probabilistic Safety Assessment

This analysis covers the BWRX-300 risk associated with shutdown and refuelling operation. The systems modelled are evaluated based on anticipated activities associated with shutdown and refuelling operations. During shutdown, the requirement for and availability of frontline and support systems will vary. Planned maintenance will also impact system availability during these operation modes. To develop a suitable PSA model, multiple bounding plant configurations are defined with similar characteristics in relation to the residual heat, the availability of systems, and the reactor vessel water levels.

The approach for the LPSD PSA is similar to the FPIE PSA, involving fault trees and event trees used in determining the shutdown risk for each IE analysed. Loss of the SDC is investigated, in addition to all IEs identified for full power which are also applicable for LPSD. An initiating event fault tree was developed to quantify the loss of SDC.

Differences between the low-power and shutdown PSA and the power operation PSA are attributed to:

- Plant operating mode
- Plant operating state including configuration
- Time after shutdown
- Reactor vessel and containment status
- Vessel and core temperatures
- Fuel location
- Availability of required systems and support systems

15.6.1.8.1 Plant Operating States

The outage plant operating mode and POS are used to define the initial plant conditions for individual ES quantification. The evaluation encompasses plant operation in hot shutdown, cold shutdown, and refuelling modes (Modes 3, 4, 5, and 6) while Mode 2 is bounded by the at-power PSA model (as shown in Table 15.6- 2) and discussed in Section 15.6.1.1. During these modes, the plant is transitioned through several plant operating states that are distinguished in the LPSD PSA by different plant conditions and configurations. The LPSD PSA addresses plant operating states where there is fuel in the reactor vessel.

This analysis defines four shutdown POSs: POS 3&4, 5, 6-1 and 6-2. Once the outage POSs are defined, the duration of each is estimated to determine its contribution to the overall calculation of annual CDF.

POS 3&4 is characterised by the following:

- Control rods are fully inserted to maintain the reactor at subcritical state.
- Decay heat can be removed by one train of SDC in this POS. LPSD POS starts when the main condenser vacuum is lost. The main condenser vacuum is lost 6 hours after the SCRAM. Each train of SDC is capable of removing 100% of the decay heat after 4 hours following reactor shutdown.
- Reactor and containment are fully tensioned. The containment is de-inerted.
- RPV water level is around the RPV head flange. In such condition, the reactor head vent line may be opened. When boil-off event occurs and ICS is used for decay heat removal, the head vent line needs to stay open for a while to allow the inventory to boil down to the ICS steam inlets and then needs to be closed in order to allow the reactor vessel to pressurise. This pressurisation will allow for the ICS to be utilized.

POS 5 is characterised by the following:

- Control rods are fully inserted to maintain the reactor at subcritical state.
- Decay heat can be removed by one train of SDC.
- Reactor is fully tensioned.
- Containment boundary is not intact.
- RPV water level is around the RPV head flange.

POS 6-1 is characterised by the following:

- Control rods are fully inserted to maintain the reactor at subcritical state
- Decay heat can be removed by one train of SDC
- Reactor is de-tensioned. (one or more RPV head closure studs are less than fully
- Tensioned)
- Containment boundary is not intact
- The reactor cavity is drained

POS 6-2 is characterised by the following:

- Control rods are fully inserted to maintain the reactor at subcritical state
- For decay heat removal function, Fuel Pool Cooling and Cleanup System (FPC) is available in addition to SDC since the fuel pool gate is open. In this POS analysis, POS 6-2 is not sub-divided by success criteria of decay heat removal since design calculation for decay heat removal is not available yet
- Reactor is de-tensioned
- Containment boundary is not intact
- The reactor cavity is flooded
- The fuel pool gate is open

15.6.1.8.2 Accident Sequence Analysis

The event sequence analysis and end state nomenclature are the same as the full power PSA. The critical safety functions credited in the shutdown model are decay heat removal, inventory control and pressure control. The containment function is credited for POSs where containment is not open. Reactivity control is assumed to have no significant effect on the shutdown model. The systems that are credited in the LPSD PSA for each safety function are summarised in Table 15.6- 4.

The associated success criteria analysis is performed in a similar way to the full power success criteria analysis. However, success criteria analysis for low power shutdown is often simpler than full power and can be approximated by hand calculations in many cases.

The following event trees were developed:

- T-GEN (General Transient)
- ELOCA (Excessive Loss of Coolant Accident)
- LLOCA (Large Loss of Coolant Accident)
- MLOCA (Medium Loss of Coolant Accident)
- SLOCA (Small Loss of Coolant Accident)

It is noted that different trees are developed for the different plant states as required.

A general transient is defined as an event that disrupts the normal operation of the plant. In the full power PSA, this would most likely be a turbine trip or scram. In the LPSD PSA, normal operations are defined as the reactor shut down and cooled by SDC. An event that disrupts such LPSD normal operation is considered in this event tree, including all initiating events that results in loss of SDC. These initiating events include loss of SDC, loss of offsite power, loss of medium voltage Alternating Current (AC) bus, loss of low voltage AC bus, loss of plant cooling water and loss of plant pneumatics. Heavy load drop initiating events that impact operating train of SDC is also modelled in this event tree. The large LOCA event also includes heavy load drop initiators. (Heavy load drop analysis is discussed more in Section 15.6.2.4)

15.6.1.8.3 System Analysis

The necessary fault trees are identified following construction of the event trees. These fault trees represent the nodes included in the event trees and any required support system fault trees.

Maximum use is made of the fault trees developed for the full power PSA. Potential differences between the at-power and the shutdown fault tree models may result from differences in:

- Maintenance unavailabilities
- Success criteria between at-power and shutdown condition
- Initial system configuration between at-power and shutdown condition
- Human actions

New fault trees are developed for the following systems that are credited in the LPSD PSA and not the full power PSA.

15.6.1.8.4 Shutdown Cooling System

The SDC system provides long term decay heat removal during shutdown phases of operation. SDC consists of two independent trains designated as Train A and Train B. Each train suction is independently connected to an ICS condensate return line outside containment, downstream of the containment isolation valves.

15.6.1.8.5 Liquid Waste Management System

The Liquid Waste Management System (LWM) system cleans liquid waste collected from plant areas via the equipment and floor drain system. The LWM system also filters, stores, and refills the reactor cavity water volume during refuelling operations.

The LWM system is divided into four subsystems:

- Condensate storage and transfer subsystem
- Waste collection and filtering subsystem
- Waste sampling subsystem
- Refuelling water storage and cleanup subsystem

The function of the LWM system as modelled in the LPSD PSA is to provide water makeup to the reactor cavity by the refuelling water storage and cleanup subsystem. The condensate storage and transfer subsystem provide water source of Condensate Storage Tank (CST) for the CRD system. CRD is credited as water makeup function for the reactor as well as purge water supply function to SDC in the LPSD PSA.

15.6.1.8.6 Water Transfer from Equipment Pool to Reactor Cavity

The function as modelled in the LPSD PSA is the transfer of water from the equipment pool to the reactor cavity. During Mode 6 of the plant operation where the spent fuel pool gate and the equipment pool gate are installed, if only SDC is lost, then CRD system purge flow will continually supply makeup to the reactor cavity as the boil-off occurs. In an event where SDC and CRD are both lost, RPV water level will boil off to Top of Active Fuel if no additional water is added. Another source of water will be necessary to flood the RPV. There are multiple backup sources to consider for an injection source to the RPV. These include firewater, ICS pools, external sources pumped through CRD piping, demineralised water, condensate storage, and the equipment pool. The preferred source is one that could be available without electric power. Therefore, the equipment pool water source is the most feasible method to utilize to provide inventory to the reactor cavity in the loss of SDC and CRD event.

15.6.1.8.7 Flexible Mitigation Capability/Emergency Mitigating Equipment

The function of Flexible Mitigation Capability (FLEX) / Mitigating Equipment (EME) as modelled in the LPSD PSA is to provide water makeup to the reactor. During low power and shutdown operation of the plant, long term loss of SDC can be mitigated by use of CRD purge injection. Long term loss of both SDC and CRD can utilize several sources of water for RPV makeup including the CST, the refuelling water storage tank, or the demineralised water storage tank.

15.6.1.8.8 Fire Protection System

The function of the Fire Protection System (FPS) as modelled in the LPSD PSA is to provide water makeup to the spent fuel pool, when the RPV head is open and fuel pool gate is open. The FPS consists of firewater storage tanks, fire pumps (2 electrical and 1 diesel) and firewater supply piping. Two dedicated firewater storage tanks are provided, one primary and the other secondary.

15.6.1.8.9 Quantification

The model development and quantification are performed using CAFTA, PRAQuant and FTREX in a similar manner to the full power PSA.

All shutdown core damage sequences lead directly to radionuclides release to the environment (containment is assumed to be open at the time of the IE). In the final PSA, this assumption will be revisited to accurately assess the Level 2 PSA results.

15.6.1.9 Spent Fuel Pool PSA

Spent fuel damage evaluation is required for the plant-specific BWRX-300 PSA because fuel damage frequency is an important contributor to release risk relative to other low risk contributors. For accidents, where the spent fuel is damaged outside the reactor core, the term fuel damage is applied, and the fuel damage frequency may be an important contributor to release risk. The term “fuel damage” represents damage to the fuel outside the reactor vessel, while “core damage” is used for damage inside the vessel.

A separate PSA analysis investigates the ESs leading to spent fuel damage. The analysis estimates the related ESs and their frequencies, and it is documented separately as part of the PSA. The analysis covers both power operation and outages. Malicious activity is explicitly excluded from the calculation of the spent fuel damage frequency.

The overall process of event tree analysis, success criteria analysis, and fault tree analysis, is the same process used in the LPSD PSA. Generally, the time available for responding to a fuel pool IE is much longer than the LPSD IE response. ESs are developed and quantified that credit potential recovery actions taken by the operator.

Three operating states are modelled for the Spent Fuel Pool (SFP) PSA:

- POS 1 - SFP gate is installed, total reactor core is NOT offloaded into the SFP
- POS 2 - SFP gate is removed connecting the reactor well and the SFP
- POS 3 - SFP gate is installed, total reactor core is offloaded into the SFP. This is assumed to occur only during a refuelling and maintenance outage every 10 years

The systems credited in the SFP PSA to support pool cooling and make-up are as follows:

- FPC
- PCW system
- LWM system
- Plant pneumatics system
- Fire protection system
- Safety Class 2 and 3 electrical distribution system

Initiating events from the FPIE analysis were screened for the impact on the SFP. Events from NUREG-1738, “Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Plants,” (Reference 15.6-45), were also considered.

Three event trees were developed to model the loss of spent fuel pool cooling: one for each of the operating states. The identified initiators were all captured as part of this IE group:

- Loss of offsite power
- Loss of PCW
- Loss of AC power
- Loss of DC power
- Loss of SFP cooling

Six operator actions were modelled, covering all POS, and enabling alternate cooling/injection on loss of cooling or start-up of the standby FPC train.

It is noted that the fire PSA for the SFP is yet to be developed. In addition, structural failure of the SFP due to seismic events, aircraft impact and tornado missiles is yet to be assessed.

Loss of coolant inventory (excluding structural failures) is screened out on the basis of low frequency, given the long-time available to make up any water loss.

Event sequences were then qualitatively analysed to determine which sequences would lead to spent fuel damage end states. The sequences are grouped together based upon the available time to prevent spent fuel damage and on release of radionuclides inside the reactor building.

The end state groups are defined as follows:

- OK: No fuel damage and no release to the reactor building environment
- BOIL: The fuel is kept intact but radionuclides in the SFP water are released to the reactor building environment due to boiling as a result of inadequate SFP cooling. Note: BOIL sequences were identified in the event trees, but not yet quantified
- SFD: spent fuel damage occurs

For the SFP PSA, it is assumed that all fuel damage events result in a large release and no credit is being taken for containing the release within the SFP enclosure.

15.6.1.9.1 Task Outputs and Preliminary Results

This task develops the spent fuel damage PSA model. The outputs of this task include:

- A screening analysis for the identification of IEs applicable to spent fuel damage
- Qualitative assessments supporting the screening analysis
- Spent fuel damage event trees for unscreened IEs
- Spent fuel damage system models
- Quantitative assessment for unscreened IEs and their associated event trees and system models
- Key risk insights and assumptions which are discussed further in Sections 15.6.6 and 15.6.8

15.6.2 Internal And External Hazard Events

The internal and external hazards portion of the PSA analyses radionuclide release accidents initiated during power operation for the following hazards:

- Internal flooding
- Internal fire
- Seismic
- High winds
- Heavy load drop

For LPSD operation, hazard events from heavy load drops have been considered. As the PSA matures, the scope of the hazards modelling will be reviewed and developed.

15.6.2.1 Internal Hazards

This section summarises the screening for internal hazards for the BWRX-300 plant. Internal hazards were screened for both consideration in the PSA and for inclusion in the fault list. In addition, potential non-reactor sources of radioactivity are screened in this section.

From IAEA SSG-64, “Protection Against Internal Hazards in the Design of Nuclear Power Plants,” (Reference 15.6-46), “Internal hazards are those hazards to the safety of the nuclear power plant that originate from within the site boundary and are associated with failures of facilities and activities that are under the control of the operating organization.”

This section documents the screening of internal hazards for the BWRX-300 Standard Plant Design (SPD). Because the BWRX-300 PSA is an all-hazards PSA, internal hazards are evaluated for potential PSA development. The methodology report, 006N2915 (Reference 15.6-9), includes guidance for screening external hazards and this screening approach can be adopted for screening internal hazards. A summary of the overall process for selection, screening and analysis of hazards is provided in Figure 15.6- 3: Overall Process for Selection, Screening and Analysis of Hazards

. The PRA Standard, ANS/ASME RA-S-1.1-2022, (Reference 15.6-14), Sections 1 and 6, also provide several screening criteria.

The general approach screens internal hazards using the following steps:

1. Develop a list of candidate internal hazards
2. Apply qualitative screening criteria to each of the internal hazards
3. For those internal hazards remaining unscreened (i.e., pose a credible threat to nuclear safety) from Step 2, consider application of quantitative screening
4. Any hazards left unscreened after Step 3 are retained as candidates for explicit treatment in the PSA

In addition, on-site radioactivity sources are screened for potential treatment in the PSA. This section on internal hazards is preliminary and will be updated as the conceptual design evolves.

15.6.2.1.1 Scope

The internal hazard scoping assessment applies screening criteria to all hazards originating within the site boundary. Several sources are consulted for developing the internal hazards list. A list of on-site radioactivity sources is considered for treatment in the PSA.

Because the BWRX-300 uses a standard plant design and because internal hazards apply to those originating within the site boundary, this screening section is applicable for all potential sites.

15.6.2.1.2 Assumptions

- Administrative controls are implemented to preclude compressed gas cylinders from becoming missiles in areas containing risk-significant mitigating equipment.
- Valves are designed to prevent removable parts from becoming missiles in the event of failure in accordance with guidance in IAEA SSG-64.
- Rotating equipment (excluding the main turbine) is designed such that potential failure-generated missiles are prevented from impacting risk-significant equipment through spatial or engineered means.
- Administrative controls are placed to ensure stored combustibles are not collected in sufficient quantities to impact nuclear safety if ignited.
- No risk-significant mitigating equipment resides in the RB Plant Services Area truck bay or the service bay area beneath the truck bay.
- The on-site radwaste system does not contain radioactivity in sufficient form or quantity to pose a public health hazard to the level of a small or large release as defined by the PSA. (Note this will be re-assessed as part of the Level 3 PSA development).
- Dry casks containing spent fuel, when stored or handled outside the cask pit, are capable of passive cooling and are not vulnerable to potential hazards.

15.6.2.1.3 Hazard List

The preliminary list of BWRX-300 internal hazards is generated from industry guidelines, past studies, and a plant-specific review.

The internal hazards list of sources includes:

- GEH, “BWRX-300 Safety Strategy,” 006N5064 (Reference 15.6-11)
- ASME/ANS RA-S-1.1-2022 (Reference 15.6-14). This source is an aggregation of hazards based on review of industry studies such as NUREG/CR-2300, NUREG-1407, IAEA SSG-3, NUREG/CR-5042, EPRI 1022997, EPRI 3002005287, and ASAMPSA_E List of External Hazards
- IAEA SSG-3 “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants,” (Reference 15.6-47).
- IAEA SSG-64 (Reference 15.6-46)

Following a review of these sources, a list of internal hazards for consideration was generated and was then subject to screening as is described in the next section.

15.6.2.1.4 Qualitative Screening

As set out in the PSA Methodology Report, 006N2915 (Reference 15.6-9), the following criteria are provided for qualitative screening of internal hazards. It is noted the screening criteria mentioned are also considered applicable to external hazards:

- The event is of equal or lesser damage potential than events for which the plant is designed. This requires an evaluation of the plant design basis to estimate the resistance to a particular (internal) event.
- The event has a significantly lower mean frequency of occurrence than similar events included in the PSA and could not result in worse consequences in those events.

- The event cannot occur close enough to the plant to affect it.
- The event is included in the definition of another event.
- The event frequency is sufficiently low compared with the probabilistic limits defined for the release category frequencies so that it does not need to be included in the PSA.

The following additional qualitative screening criteria, from ASME/ANS RA-S-1.1-2022 (Reference 15.6-14) are also considered:

- The event does not result in a plant trip (manual or automatic) or require a plant shutdown.
- The event develops slowly, and it is shown there is demonstrably conservative time margin available to eliminate the source or to provide adequate response.

The following events were assessed qualitatively:

- Heavy load drop
- Release of chemicals from on-site storage
- Turbine-generated missiles
- Other internally generated missiles (i.e., from pressure vessels, valve failures, control rods and high-speed equipment other than turbine generated missiles)
- Explosions
- Collapse of structures
- Pipe whips
- Jet effects

Internal fire and internal flooding hazards are not subject to screening and are taken forward for further analysis in the PSA.

15.6.2.1.5 Quantitative Screening

The quantitative screening criteria from RA-S-1.4-2021, “Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants,” (Reference 15.6-48) are applied for internal hazards. It is noted, the same criteria are applicable to external hazards. A hazard screens quantitatively if:

- Based on absolute risk contribution, an event sequence family subject to screening does not exceed the selected risk significance criteria and has mean occurrence frequencies less than 1E-7/plant-year, as estimated using a bounding or demonstrably conservative analysis.
- The total contribution of all screened out event sequence families does not exceed 1% of the cumulative risk targets included in the absolute risk significance criteria.

The following events were assessed quantitatively:

- Turbine-generated missiles

A summary of the internal hazards screened out from further analysis and those taken forward to be assessed further in the PSA are presented in Table 15.6- 5: Summary of Internal Hazards Screening to Determine Internal Hazards Taken Forward for Further Evaluation in the PSA.

15.6.2.2 Internal Fire Hazard

The probabilistic fire analysis is performed with simplifying assumptions because the specifics of cable routings, ignition sources, or target locations in each zone of the plant are still in the design phase. Due to this limitation, a simplified, conservative, and bounding approach is used in this analysis. The current scope of the analysis is to address At-power plant operations. This will involve aspects such as plant partitioning of the global plant analysis boundary into Physical Analysis Units (PAU), component/cable selection, estimation of fire ignition frequency, fire failure analysis and development of the fire-induced risk model. The aim being to calculate the internal fire-induced CDF and LRF using internal fire frequencies developed and fire-specific conditional damage probability factors. The full approach and output of the internal fire analysis is described in the following sections.

15.6.2.2.1 Methodology

The BWRX-300 internal fire PSA is performed according to the guidance in NUREG/CR-6850, EPRI 1011989, EPRI/NRC-RES “Fire PRA Methodology for Nuclear Power Facilities,” (Reference 15.6-49), as applicable.

State-of-the-art modelling methods, tools, and data for conducting a commercial nuclear power plant fire PSA are presented in NUREG/CR-6850, EPRI 1011989 (Reference 15.6-49) and NUREG/CR-6850 Supplement 1, EPRI 1019259, “Fire Probabilistic Risk Assessment Methods Enhancements,” (Reference 15.6-50). The methods have been developed under the fire risk re-quantification study. This study was conducted as a joint activity between the EPRI and the U.S. NRC Office of Nuclear Regulatory Research under the terms of an NRC/EPRI Memorandum of Understanding and an accompanying Fire Research Addendum.

For the BWRX-300 Fire PSA model development, the following NUREG/CR-6850 EPRI 1011989 (Reference 15.6-49) and NUREG/CR-6850 Supplement 1, EPRI 1019259 (Reference 15.6-50), tasks are applicable:

- Task 1: Plant Boundary & Partitioning
- Task 2: Fire PSA Component Selection
- Task 3: Fire PSA Cable Selection
- Task 4: Qualitative Screening
- Task 5: Fire-Induced Risk Model
- Task 6: Fire Ignition Frequencies
- Task 7: Quantitative Screening
- Task 8: Scoping Fire Modelling
- Task 12: Post-Fire Human Reliability Analysis
- Task 14: Fire Risk Quantification
- Task 15: Uncertainty and Sensitivity Analyses
- Task 16: Fire PSA Documentation

Some of the above tasks are performed with simplification while others are omitted at this stage of the BWRX-300 Fire PSA due to the maturity of the plant design, see FAP item PSR15.6 – 47 in Appendix B. Tasks not addressed in this study since the BWRX-300 plant is still in the design phase include: (a) Detailed Circuit Failure Analysis (Task 9); (b) Detailed Circuit Failure Mode and Likelihood (Task 10); (c) Detailed Fire Modelling (Task 11) including Main Control Room (MCR) and Multi-Compartment analysis; (d) Seismic-Fire Interaction (Task 13); and (e) Support Task A, Plant Walk Downs.

Support Task B, Fire PSA Database, is performed with an Access®-driven database (FRANX) that includes all tables that are necessary to develop a scoping-level fire PSA model. Enhancements to the fire PSA database are possible in future updates once more details are available for cable tray routes and their contents as well as more detailed ignition source locations.

Fire ignition frequencies for power operation at each plant area PAU are estimated using the NUREG/CR-6850, EPRI 1011989 (Reference 15.6-49) and NUREG/CR-6850, EPRI 1019259, Supplement 1 (Reference 15.6-50) methodology and data from NUREG-2169, EPRI 3002002936 “Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database”, (Reference 15.6-51) and NUREG-2230, EPRI 3002016051 “Methodology for Modelling Fire Growth and Suppression Response for Electrical Cabinet Fires in Nuclear Power Plants,” (Reference 15.6-52). Fire frequencies for shutdown conditions are not developed at this time.

For a postulated fire, a list of the impacted components is generated with the mapping defined in the fire PSA database. A list of impacted components is also generated with the assumed cable routing. The cable routing is assumed based on the modelled PSA components, their supports, and the general room layout of the BWRX-300 design. Fires are conservatively assumed to propagate unmitigated in each PAU (no suppression is credited) and damage all functions in the PAU. The internal events PSA accident sequence structures and system fault trees and success criteria are used in the calculation of the fire CDF and LRF.

The BWRX-300 fire PSA employs the following EPRI software:

- FRANX, uses the internal events model and adds fire initiators
- FTREX, generates cutsets from the fault trees produced in CAFTA
- CAFTA, is used to build the logic model of the plant, producing all the fault trees and event trees

15.6.2.2.2 Fire Ignition Frequency

This section outlines the steps involved in calculating the fire ignition frequency during At-power operations for each of the unscreened fire areas of this analysis. The NUREG/CR-6850, EPRI 1011989 (Reference 15.6-49) and NUREG/CR-6850 Supplement 1, EPRI 1019259 (Reference 15.6-50) methodology was used to calculate the full-power fire ignition frequencies using generic data from NUREG-2169, EPRI 3002002936 (Reference 15.6-51). NUREG-2169 is used as the frequency source for all ignition source bins except for Bin15 (Electrical Cabinets), for which NUREG-2230 (Reference 15.6-52) is used.

This task was organized around the following eight steps:

- Step 1: Mapping plant ignition sources to generic sources
- Step 2: Plant fire event data collection and review
- Step 3: Plant-specific updates of generic ignition frequencies
- Step 4: Mapping plant-specific locations to generic locations
- Step 5: Location weighting factors
- Step 6: Fixed fire ignition source counts
- Step 7: Ignition source weighting factors
- Step 8: Ignition source and compartment fire frequency evaluation

It is noted Steps 2 and 3 are not applicable at this stage since the BWRX-300 plant is in the design phase. The location weighting factors are simplified as described in the assumptions below.

15.6.2.2.3 Detailed Fire Modelling

Single compartment and MCR detailed fire modelling are not performed for this version of the BWRX-300 Fire PSA for at-power operation. Detailed fire modelling can be undertaken when the BWRX-300 design is more complete and additional details on equipment location and cable tray routes are known with certainty.

In this version of the internal fire PSA, full room PAU burnout scenarios are used where any PSA related component and cable within the particular PAU is failed, at the total PAU ignition frequency.

Fire propagation cases (multi-compartment analysis scenarios) that involve spread from one PAU into another PAU are not currently postulated for the fire areas listed in the at-power fire PSA. As the BWRX-300 design matures with greater detail, this analysis will be undertaken.

Detailed HVS design information is not yet available for the BWRX-300 plant design; therefore, consequential failures from potential smoke damage cannot be assessed. This is subject to future updates of the internal fire PSA as the plant design matures. The fire PSA models full burnup of the PAU in which the fire originates and therefore implicitly addresses potential smoke damage that could occur in that PAU.

The shutdown fire PSA model is not yet constructed but is expected to be based on the Level 1 internal events shutdown PSA model. Detailed shutdown fire modelling will follow the same process as described above except the evaluation of the applicability of shutdown conditions to the fire PSA model in future updates of the internal fire PSA.

15.6.2.2.4 Key Inputs and Assumptions

The following are the inputs for the BWRX-300 fire analysis:

- FPIE PSA model
- Fire compartment spatial information

The fire risk analysis is performed using simplifying and conservative assumptions due, in part, to the stage of the design. The key conservative assumptions are summarised below:

- A fire ignition in any fire area may grow into a fully developed fire.
- The analysis does not take credit for any fire suppression (i.e., self-extinguishment, installed suppression systems, nor manual firefighting activities). Therefore, the analysis assumes that all fires disable all potentially affected equipment in the area.
- Unless otherwise stated, a fire is assumed to cause failure of all fire-susceptible components in the subject fire area and detailed fire modelling is not performed in this revision of the BWRX-300 Fire PSA.
- Recovery of the failed components or cables after the postulated fire is not credited.
- Unless otherwise stated, the analysis does not take credit for the distance between fire sources and targets.
- The analysis assumes that all fire-induced equipment damage occurs at a time of zero in the scenario progression.
- Based on the plant general arrangement drawings with component locations, assumed cable routing is postulated for PSA purposes. Note that there are no details for cable routing in the BWRX-300 plant design at the time of this analysis beyond locations of some of the major electrical system components. A list of cables is generated that includes all modelled supports for PSA components included in the current at-power internal events PSA model. This list captures most cables, especially for expected risk-significant components.

- Fires in the MCR and Secondary Control Room (SCR) are currently modelled as impacting components associated with any assumed cable routings that go through the rooms but do not terminate in the MCR or SCR. The MCR and SCR are not assumed to impact components for which control or visualization cables that may be in the rooms. This is likely a realistic treatment, as the plant design could be similar to other BWR designs, in which control room controls are connected to the DCIS rooms (which are unaffected by a MCR fire) via fibre cables. The loss, including melting, of the fibres or visual display units does not cause inadvertent actuations, nor affect the automatic actuations associated with safety class and non-safety class equipment. In addition, fires in the MCR and SCR are assumed to fail all modelled HFEs.
- All finalised details of cable route information are assumed to be not yet available. Individual routes are assumed based on location of PSA modelled power/signal sources and the particular component.
- Fire ignition frequencies remain constant over time and are based on industry generic fire frequencies. Among the operating plants, total ignition frequency is the same between plants for the same equipment type, regardless of differences in the quantity and characteristics of the equipment type that may exist among the plants. This is likely conservative since the BWRX-300 design has significantly lower numbers of pumps, motors, and other active components than earlier plant designs on which the current generic ignition frequencies are based on. It is assumed that all ignition source type bins are applicable to the BWRX-300 plant with the following exceptions:
    - Bins 02 and 03 are not applicable since they are used for Pressurised Water Reactor plant designs.
    - Bin 22 for RPS motor generator sets is not applicable to BWRX-300 plants since it is typically a Pressurised Water Reactor plant feature.
    - Bin 04 is likely not applicable to the BWRX-300 MCR or SCR as the BWRX-300 design is completely digital as opposed to traditional electro-mechanical designs. However, to ensure a conservative analysis is produced, twenty-five percent (25%) of the traditional Bin 04 ignition frequency is assumed to be applicable and is assigned to the BWRX-300 MCR ignition frequency.
- Since the BWRX-300 plant is still in design phase, the count of components is performed with the modelled PSA components as well as preliminary design layout drawings.
- Since the plant has not operated and no history of maintenance activity is available, the weighting factor evaluation is simplified. It is assumed that all compartment PAUs have the same transient fire influencing factors; a value of one is used for all influencing factors.
- All fires are assumed to result in a manual reactor shutdown regardless of location or potential induced failures.
- Full details of electrical cabinet locations are not yet available. Preliminary design information which notes the division or train of equipment is used in the development of this revision of the BWRX-300 Internal Fire PSA for electrical cabinet and high energy arching fault counts. Note that some of these counts are assumptions with engineering judgment for typical nuclear plant layouts and functions.
- Some components remain unlocated due to the preliminary design of the BWRX-300 plant. These components are assigned to a location zone of “UNL” (unknown location) in the analysis. The UNL zone is failed for all quantified scenarios, serving to fail any unlocated components for all scenarios. This is conservative since the components

are impacted for many scenario locations that are not expected to impact the components once detailed location information and any applicable cable routing is finalised. The "UNL" zone is failed in the Fire PRA model database scenario list in that the zone names impacted for each scenario are listed in the Fire PRA model database table "Zone to Raceway" that has the zone names and components that are impacted for the particular zone name. The component names are mapped to PSA model BEs which are failed during the fire PSA model quantification.

Task Outputs and Preliminary Results

FRANX and FTREX were used to quantify the CDF and LRF results for each fire scenario, as well as grouped cutsets allowing evaluation of total CDF and LRF.

The following tasks have been completed:

- At-power fire PSA model has been created
- Key PSA assumptions and modelling approaches have been reported
- Description of the partitioning of the plant into fire compartments
- Description of the specific methods and data used for assessing the fire hazard
- Specific changes made in the Level 1 PSA model for internal IEs aimed to account for the effects of internal fire
- Characterisation of fire compartments
- Justification for the screening of particular fire compartments from the analysis
- The final results of the Level 1 PSA for internal fire in terms of CDF and LRF

15.6.2.3 Internal Flooding Hazard

The objectives of the BWRX-300 internal probabilistic flood analysis are to identify and provide a quantitative assessment of the radionuclide release risk due to internal flood events. It models potential flood vulnerabilities, in conjunction with random failures modelled as part of the internal events PSA. Through this process, flood vulnerabilities that could jeopardize core integrity and containment integrity are identified. The current scope of the analysis is to address at-power plant operations and derive the CDF for this hazard. The FPIE model is used as the base model for the development of the internal flooding PSA.

Floods may be caused by large leaks due to rupture or cracking of pipes, piping components, or water/fluid containers such as storage tanks. Another possible flooding cause is the operation of fire protection equipment.

Flooding associated from external sources such as localized flooding events and intense weather events (considered under the External Flooding Hazard Analysis) are excluded from this analysis.

15.6.2.3.1 Methodology

The internal PSA flooding analysis is conducted by identifying and classifying potential flooding sources and events. Component location and data is compiled to generate a frequency of occurrence to represent the effects associated with each of the potential flooding events. In addition, an evaluation is performed to identify, screen, and quantify specific plant effects/failures associated with each flooding event. Finally, the BWRX-300-specific flooding frequencies and plant effects are applied to the PSA model to obtain risk results. For the BWRX-300 Flooding PSA model development, the following tasks are performed:

- Define global assessment boundary, plant partitioning and component selection
- Identification of flood sources and component locations

- Development of flooding scenarios
- Development of flooding frequencies
- Plant response analysis
- Analysis of flooding scenarios

The internal PSA flooding analysis is based on the design basis for the BWRX-300 SSCs. The location of these features and their interaction with other BWRX-300 SCCs and equipment is critical to the flooding analysis. The current list of system components and location of equipment is assumed based on the current design and plant layout drawings and relies on the component location analysis performed for the fire PSA step (e.g., common spatial information).

The development of BWRX-300-specific flooding scenarios requires a detailed analysis of data including plant component location, system capacity, and potential failure mechanisms. Characteristic scenarios are selected as representative of flood areas and subject to quantitative analysis following the identification of potential flooding scenarios.

In order to develop the severity and effect of potential flooding scenarios, data is collected from industry sources (NUREG/CR-6928 (Reference 15.6-28), Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants) for the BWRX-300 equipment and system components. Failure data for consideration in the flooding analysis includes piping runs, pumps, valves, tanks, heat exchangers, and circulating water expansion joints. These failure rates in combination with types and capacity of system components located within specific flood zones are used to develop the flooding frequencies and frequency uncertainties. Flooding frequencies for both large break and small leak scenarios are developed for each flooding scenario. Finally, the flood scenarios for each flood area are quantified to calculate a probabilistic risk value and summed to provide an overall risk analysis for the BWRX-300.

NUREG/CR-4639, “Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR),” provides additional guidance for flooding analysis (Reference 15.6-53). The requirements for a flooding PSA are discussed in ASME/ANS RA-S-1.1-2022 (Reference 15.6-14), Part 4.

Walkdowns are a critical task for a mature flooding PSA and will be performed and documented after the construction of the plant has been completed.

The BWRX-300 Internal Flooding PSA employs the following software for model development and quantification:

- FRANX, uses the internal events model and adds high wind initiators.
- FTREX, generates cutsets from the fault trees produced in CAFTA
- CAFTA, is used to build the logic model of the plant, producing all the fault trees and event trees.
- ACUBE, this software provides a more accurate solution to the cutsets than conventional solutions

15.6.2.3.2 Key Inputs and Assumptions

The following are the inputs for the BWRX-300 internal PSA flooding analysis:

- FPIE PSA model
- BWRX-300 design features for protection against flooding
- Flood zone spatial information

The key assumptions used in support of the BWRX-300 flooding analysis are summarised below:

- Flooding resulting from component ruptures considered in this analysis
- For each tank rupture, the entire tank inventory is drained
- Non-qualified equipment (motors or solenoids for valves, control cabinets and circuitry) affected by submergence is assumed to fail if the water level in the flood zone reaches a level of 0.5ft above floor elevation or if sprayed
- If equipment is failed by the flooding event in the source location or along the propagation pathway, it is assumed the equipment is failed at the start of the flood
- The expected effect of flooding electrical equipment such as MCCs, electrical cabinets, and terminal boxes, is a short to ground, removing power from the loads served by the component. This analysis addresses all such failures of electrical equipment as ground shorts
- MOVs require the application of current to the motor to change the valve position. Without power, the valve remains in its current position. Flooding and/or spraying of a MOV causes the valve to fail as-is
- Passive components, such as pipes, heat exchangers, and tanks are not considered to be vulnerable to flooding effects because of the passive nature of the components Buoyancy or impactive force from the flooding source water is not analysed or considered for potential failures of SSCs in this revision of the BWRX-300 Internal Flood PSA
- Water collecting in a stairwell or propagating into a stairwell preferentially continues to travel down the stairwell as opposed to propagating under a door adjacent to the stairwell
- The mission time of the active equipment credited in the flooding risk analysis will be 24 hours, unless a shorter mission time is specified by analysis, or a longer-term mission time is needed to ensure the plant is safe-and-stable. This is the same as the internal events PSA.
- The internal flooding analysis uses the same systemic success criteria as used in the internal events PSA
- Fire doors are not watertight
- Concrete walls are considered flood barriers. Concrete walls are assumed to be capable of withstanding the expected maximum flood loading and are assumed to remain intact throughout a flooding event.
- The analysis does not take credit for any mitigation of the flooding event by operators or automatic system functions. Therefore, the analysis assumes that all floods disable all potentially affected equipment in the areas where the flood is postulated to propagate, see FAP item PSR15.6 – 46 in Appendix B.
- Recovery of the failed components after the postulated flood is not credited
- Based on the plant general arrangement drawings with component locations, assumed pipe routing is postulated for PSA purposes. Note that there are no details for pipe routing in the BWRX-300 plant design for plant systems at the time of this analysis beyond locations of some of the major system components.
- Some components remain unlocated due to the preliminary design of the BWRX-300 plant. These components are assigned to a location zone of “UNL” in the analysis. The

UNL zone is failed for all quantified scenarios, serving to fail any UNL components for all scenarios. This is conservative since the components are impacted for all scenario locations, many of which would not be expected to impact the components once detailed location information is finalised. The “UNL” zone is failed in the internal flood PSA model database scenario list in which the zone names impacted for each scenario are listed in the internal flood PSA model database table “Zone to Raceway” which has the zone names and which components are impacted for the particular zone name. The component names are mapped to PSA model basic events which are failed during the internal flood PSA model quantification.

- Flood events inside the primary containment are not analysed in this flooding analysis as those events are modelled in the LOCA analysis.

15.6.2.3.3 Task Outputs and Preliminary Results

The internal flood PSA CDF has been derived. The LRF is reported to be the same as CDF at this stage, with all core damage sequences treated as going straight to large release. The Level 2 analysis will be developed at a future point. For CDF, each individual internal flood scenario has been quantified along with the grouped cutset to provide the total CDF. The results have been reviewed for correctness, completeness, and consistency. Risk significant contributors and uncertainties have been documented.

The following tasks have been completed:

- At-power flooding PSA model
- Summary reports for the probabilistic internal flooding analysis
- Key PSA assumptions and insights from internal flooding analysis
- Description of the specific methods and data used to assess the internal flooding hazard
- Specific changes made to the Level 1 PSA model for internal IEs aimed at accounting for the effects of internal flooding
- Justification for the screening of particular flooding scenarios from the analysis
- Results of the detailed analysis for flooding scenarios, including scenarios, and significant assumptions made in the analysis

15.6.2.4 Heavy Load Drop

The heavy load drop assessment considers heavy loads being dropped on fuel and in other plant areas, including the spent fuel pool. Operation during both at-power and LPSD is considered. The heavy load drop damage initiator frequency is calculated and is used as input to the applicable PSA model fault tree, for example in the LPSD PSA.

The PSA analyses heavy load drops that can cause fuel damage or core damage. The heavy load drop scenarios consider drops over the spent fuel pool, the reactor vessel, fuel assemblies and other SSCs.

A screening methodology is used to identify those heavy load lifts/movements that require further risk assessment. Those lifts/movements that screen out are handled under the plant’s normal work practices and existing administrative controls.

15.6.2.4.1 Task Outputs and Preliminary Results

The following heavy load movement related initiators are evaluated in the PSA:

- Spent fuel pool leak due to rupture during at-power (Fuel Damage Frequency (FDF))
- RPV leak due to rupture (below top of fuel) during low power and shutdown (CDF)

- RPV leak due to rupture (at FW nozzle) during low power and shutdown (CDF)
- Spent fuel pool leak due to rupture during low power and shutdown (FDF)
- Loss of ICS Train A to SDC during low power and shutdown (CDF)
- Loss of ICS Train B to SDC during low power and shutdown (CDF)

For at-power operation, the risk contribution is from spent fuel damage due to cask movements leading to fuel damage. There is no heavy load drop induced core damage contribution from at-power operation. During LPSD operation, again there is fuel damage potential due to outage lifts occurring over the spent fuel pool. In addition, at LPSD, there is potential for RPV leaks (below top of fuel and at FW nozzle) and loss of either ICS Train A or B, leading to core damage. The LPSD core damage events are integrated into the LPSD PSA. For the spent fuel PSA, it is assumed that all fuel damage events result in a large release and no credit is taken for containing the release within the spent fuel pool enclosure. Similarly, for the LPSD PSA, each core damage event leads to a large release since the containment is de-inerted or open.

15.6.2.5 External Hazards

The definition of the generic site envelope and identification of credible external hazards is presented in PSR Subchapter 15.8 – External Hazards. A list of external hazard events has been developed which envelopes the potential external hazards applicable to a generic site.

A detailed description of the of the PSA approach to modelling external hazards can be found in the PSA Methodology Report, 006N2915 (Reference 15.6-9).

External hazard prioritisation and analysis has not been performed at this stage. FAP items PSR15.6 – 43 and PSR15.6 – 44 in Appendix B include the actions to perform external hazard prioritisation and hazard characterisation applicable to the site.

Hazard prioritisation will determine which external hazards, including combined hazards, need to be taken forward for PSA evaluation, either as a bounding assessment or further detailed analysis.

For illustrative purposes, the high wind and seismic hazard assessment performed for the standard plant design based on hazard characterisation suitable for North America is presented. Whilst the hazard analysis characterisation may not be specific for the future selected site; it does serve as an indicative demonstration of the application of the PSA methodology and how the external hazards analysis will be developed for two common and typically significant external hazards. Although the initial modelling is conservative, useful risk insights have been obtained from the early results.

15.6.2.5.1 Hazard Combinations

Occurrences of natural and human-induced external hazards and their credible combinations that could affect the safety of installation needs to be identified and included in the safety assessment.

The combinations of external hazards or correlated hazards are to be developed for those hazards that have the potential to combine to have a larger impact than the individual hazards and this is captured by FAP item PSR15.6 - 45 in Appendix B.

15.6.2.6 High Wind Hazard

The high wind PSA evaluates the impacts of high wind events during at-power conditions, on the safe shutdown of the BWRX-300, deriving the CDF and LRF for this hazard. The high wind analysis explicitly quantifies event sequences, and containment releases initiated by straight-line winds, tornado, and hurricane. For the accident sequence development, the high wind PSA utilises the internal events accident sequences of LOPP and LOPP-ATWS. It is noted again, this analysis is provided as a means to demonstrate how high wind hazard analysis will be developed. With this in mind, the high wind PSA described below, and the results presented are based on hazard analysis derived for a generic site in North America.

15.6.2.6.1 Methodology

The high wind risk analysis involves the following major steps:

- High wind hazard analysis
- High wind fragility analysis
- High wind plant response model development
- High wind PSA quantification

The high wind PSA is conducted by identifying and classifying potential high wind events. Data is then compiled to generate a frequency of occurrence to represent each of the potential high wind events. In addition, a qualitative evaluation of the BWRX-300 systems, structure and components is performed to identify specific plant effects/failures associated with each high wind event. Finally, a BWRX-300-specific high wind event frequency and plant effects are applied to the at-power PSA model to obtain risk results. High wind hazards are to be characterised by their impacts (e.g., dynamic load from gusts, averaged loading, rotation velocity, pressure differential, tornado path, missile impact potential).

The high winds HRA addresses modelling of human failure events for the high wind PSA. This HRA is performed to support quantification of high wind scenarios. For all human failure events in the high wind scenarios, various performance shaping factors are considered, and the human error probability is adjusted accordingly.

At-power wind-induced accident scenarios and releases are quantified and analysed. The following references provide guidance for the high wind risk analysis:

- NUREG/CR-6890, Volume 1, “Re-evaluation of Station Blackout Risk at Nuclear Power Plants Analysis of Loss of Offsite Power Events: 1986-2004,” (Reference 15.6-54)
- “Enhanced Fujita Scale (EF-Scale),” Wind Science and Engineering Center, October 10, 2006, Revision 2 (Reference 15.6-55)
- NUREG/CR-4461, “Tornado Climatology of the Contiguous United States,” Rev. 1 (Reference 15.6-56)
- EPRI 3002008092, “High Wind Equipment List and Walkdown Guidance,” December, (2016) (Reference 15.6-57)
- NUREG/CR-7004, “Technical Basis for Regulatory Guidance on Design-Basis Hurricane-Borne Missile Speeds for Nuclear Power Plants,” 2011 (Reference 15.6-58)
- NUREG/CR-7005, “Technical Basis for Regulatory Guidance on Design-Basis Hurricane Wind Speeds for Nuclear Power Plants,” 2011 (Reference 15.6-59)
- ASME/ANS RA-S-1.1 2022 (Reference 15.6-14) includes a hazard screening section (Part 6) and a high winds PSA section (Part 7). The enhanced standard, including the guidance in the non- mandatory appendix, provides requirements and guidance on performance of a detailed high winds PSA. Included in the standard requirements is the consideration of correlated hazards and hazard effects, such as the potential for local flooding associated with high winds or the impact of high wind-driven rain. This standard is utilized for both the screening of potential hazards and the analysis of any unscreened hazards.

The BWRX-300 high wind PSA employs the following software for fault tree development and quantification:

- FRANX, the high wind PSA plant response model has been produced by developing FRANX models for straight wind, tornado, and hurricane
- FTREX, generates cutsets from the fault trees produced in CAFTA
- ACUBE, is utilized in the quantification to address the overestimation of risk due to rare event approximations
- CAFTA, is used for the high wind PSA fault tree development and review of results

15.6.2.6.2 Key Inputs and Assumptions

Site-specific data are inputs for the external hazards PSA analyses. Site-specific wind hazard analysis generally requires the use of regional data. The size of the region requires judgment and depends on the regional climatology and type of wind hazard, the number of years accurate records are available, the extent and quality of the data, and the hazard's spatial variability within the region. In the design phase, it is possible to select a bounding region for a high wind hazard; however, a bounding region for tornadoes may not be the bounding region for hurricanes.

The high winds equipment list is provided by the high winds PSA documentation and is evaluated based on the internal events PSA required functions and supporting SSCs. The internal events PSA is used to quantify the high winds PSA with modification of the damaged or potentially damaged SSCs.

Below is a list of some of the key assumptions used in conducting the BWRX-300 high wind risk analysis:

- For tornado and hurricane, the contents of all BWRX-300 structures other than the RB, except for the MCR, are assumed to be unavailable given a tornado or hurricane event that strikes the site. The MCR is designed against missile penetration and missiles are assumed to not penetrate the MCR. Damage to SSCs located within these other structures could arise from pressure damage of the structures due to wind loading, wind-generated offsite and onsite missile or structural cladding failure combined with wind-driven precipitation.
- The BWRX-300 diesel generators are assumed to be air-cooled; therefore, they do not rely on PCW for cooling. However, the diesel generators have an instrument air dependency for fuel transfer, which requires cooling via PCW to support the instrument air system.
- A containment vent is currently included in the BWRX-300 design. The containment vent components are in the RB and do not extend outside of the RB envelope and are assumed to not be impacted by high wind events.
- The current average lead time for tornado warnings in the United States is 13 minutes and this average lead time is assumed to be applicable for the SPD. Given this relatively short representative lead time, for tornado events that impact the plant, operators are assumed to be in the MCR when the tornado strikes. No credit is given for advanced warning of the tornado; that is operators are assumed to have no advanced warning of the event prior to the tornado strike.
- A plant scram or manual shutdown is assumed to occur given a straight wind or hurricane event. Procedurally, it is assumed that operators are directed to shut down the plant if wind speeds at the site are measured in excess of a procedural threshold (e.g., 73 mph for U.S. nuclear plants). It is also noted that supervisory plant operators may exercise judgement in command and control by anticipatorily ordering the actions to prepare the plant for storm impacts, including any actions required to place the plant

in a safe and stable configuration, prior to reaching procedural thresholds. During tornado events, no credit is given for advanced warning of the event.

- Due to potential damage from high wind events to structure(s) housing FLEX equipment, and potential inaccessibility by operators, FLEX SSCs are assumed to be unavailable.
- Wind-driven precipitation, including rain and hail, is assumed to accompany all high wind events modelled by the high wind PSA. The consequence assessments for high wind damaged structures consider the impact of wetting from the rain and missile impacts from the hail.
- The contents of the Turbine Building, Control Building, and Intake Structure (except for the MCR, which is protected from missile penetration) are conservatively assumed to be failed by wind generated offsite and onsite missiles for tornado and hurricane. The probabilistic potential for wind-generated missile strikes is assumed to be proportional to wind speed. Missile impact probabilities for lower tornado and hurricane Wind Speed Bins (WSBs) have been assigned based on engineering judgment, considering for each WSB the likelihood of a missile of sufficient mass to be lifted and forcefully thrust into contact with applicable targets, resulting in damage.
- Warning time for hurricane events may be on the order of days or weeks. Warning time for straight wind events may be on the order of days or hours. Sufficient lead time exists for these events to prepare and plan anticipated emergency response. These actions may include procedure review, inventory of supplies, and assigned monitoring of storm progression. In the event that a severe straight wind scenario progresses relatively quickly, it is assumed that the high wind warnings or advisories (or, in the case of a derecho straight wind event, severe thunderstorm warnings) will be issued with sufficient lead time (on the order of hours) for plant operators to closely monitor site wind speeds and initiate anticipatory actions to place the plant in a safe and stable state, as necessary.

15.6.2.6.3 Task Outputs and Preliminary Results

On review of the high wind hazards, including combinations of wind hazards, a list of high wind hazards applicable to the BWRX-300 standard plant design was compiled. Based on this review of high wind hazards: straight wind, wind-driven rain, wind-driven ice, tornado, atmospheric pressure change, tornado missile, hurricane, and hurricane missile were selected for analysis. The high wind PSA was developed to model these hazards.

The wind hazard analysis derived the wind hazard frequencies for a BWRX-300 SPD. The wind hazard analysis includes the development of the high wind equipment list and development of BWRX-300 high wind component fragilities. The high wind PSA plant response model has been produced by developing FRANX models for straight wind, tornado, and hurricane. The high wind PSA FRANX models utilize the straight wind, hurricane and tornado hazard modules using the wind speed bins of standard plant design to produce Level 1 CDF and Level 2 LRF results.

The following tasks have been completed:

- At-power high wind PSA models
- Key PSA assumptions and insights from high wind analysis
- Description of the specific methods and data used for determining the hazard curves for high winds
- Specific changes made in the Level 1 PSA model to account for effects relating to high winds

- List of all SSCs considered in the analysis along with the justification for the SSCs that are screened out from the analysis
- Methodology and data used to derive wind fragilities for all SSCs modelled in the Level 1 PSA
- Final results of the Level 1 PSA in terms of core damage and large release, as well as useful intermediate results

15.6.2.7 Seismic Hazard

The BWRX-300 PSA develops Seismic Probabilistic Safety Assessment (SPSA) for at-power conditions, deriving the CDF and LRF for this hazard. The seismic analysis integrates the seismic hazard analysis, the structural/mechanical dynamic response, the component fragility, and the plant systems response. The plant operational and emergency systems are represented by event and fault trees. The analysis gives insights into the dominant contributors for the seismic risk.

For a more detailed seismic risk analysis, the scheme can be thought of as consisting of a set of analyses at each of a sequence of ground motion input levels or bins. The seismic hazard analysis provides the annual frequency of exceeding each level of peak horizontal ground acceleration. The plant components' behaviours at each level are evaluated to determine their failure probabilities. A fragility for each component, based on its design and its level in the plant is determined. HEPs are adjusted based on ground motion levels to account for increased difficulty due to seismic damage, as applicable. It is noted again, this analysis is provided as a means to demonstrate how the seismic hazard analysis will be developed. With this in mind, the SPSA described below, and the results presented are based on a hazard analysis derived for a generic site in North America.

In general terms the plant consists of normally operating and emergency standby systems and components. The failure during an earthquake (induced either directly by excessive inertial stresses or indirectly following the failure of some other item, e.g., a crane) of an operating component leads to a change in the state of the plant. In that case, various scenarios can follow depending on the "initiating" event and the status of other sub-systems. The analysis represents these possible chronological sequences by an event tree.

The event trees and the associated fault trees model the sub-systems down to the level of individual components such as pumps, valves, tanks, etc. These trees include items not found in non-seismic PSA fault trees, such as buildings whose failure induce the seismic failure of several system components. Simple combination of the frequency at each ground motion level and the two sets of probabilities (seismic input and core damage or release category frequency given the input) yields the final results.

15.6.2.7.1 Methodology

The approach used for evaluating the BWRX-300 seismic hazard and compiling the SPSA model are explained in detail in the PSA Methodology Report, 006N2915 (Reference 15.6-9). The main steps of the SPSA are as follows:

- Probabilistic seismic hazard analysis applicable to the site
- Seismic capacity and fragility evaluation of the SSCs
- Seismic plant response analysis
- Quantification and uncertainty evaluation

The seismic hazard analysis involves defining a seismic hazard frequency curve applicable to the site. The seismic hazards frequency curve provides the annual frequency of exceeding a seismic intensity.

The seismic capacity and fragility analyses involve the identification of key components and their associated capacity to withstand a seismic event.

During the plant response analysis, seismic fragility calculations are incorporated into system fault trees, and seismic event trees are developed and quantified with initiator frequencies determined from the seismic hazard analysis.

For the seismic HRA, the FRANX seismic HRA module takes existing internal events HFEs and calculates HEPs as a function of ground motion levels. This accounts for increased stress, personnel availability, and equipment accessibility by increasing the HEPs as ground acceleration increases.

Within these major steps outlined above, the contribution of seismically induced events to the plant risk is estimated using the approach outlined in the following steps:

- An estimate of seismicity of the site is characterised in terms of a seismic hazard curve.
- Event tree models are constructed to represent possible responses of systems important to safe operation or shutdown of the plant under at-power conditions following an earthquake, and to evaluate the contribution of the earthquake to plant risk.
- Seismic fault trees are constructed for the systems and structures of interest. The fault trees identify and include the structures and components in each system that are subject to functional failure as a result of an earthquake.
- Seismic fragilities are assessed for each component and structure included in the analysis.
- The fault trees and event trees are evaluated including both seismically and randomly induced failures to determine event sequence and release category frequencies. Random failures during the event sequences are determined from the internal events analysis.
- Containment event trees are then developed. These event trees draw from the insights gained in the internal events analysis to determine the system and phenomenological issues of importance. In addition, special system considerations are given to unique failure modes identified from the seismic event trees. The results are then grouped into plant damage states.
- Risk analyses are then performed using the frequencies and the consequences of each plant damage state to describe the core damage and large release frequency associated with each event tree sequence.

15.6.2.7.2 Quantification of Seismic Risk

The risk analysis is performed using the EPRI software tool FRANX. The inputs to the program are the- following:

- Seismic hazard function
- Seismic fault trees based on the internal events fault trees
- Seismic event trees
- Unavailability of systems and components that survive the seismic event (including seismic HEPs)
- Component and structural fragilities (probabilities)

The BWRX-300 SPSA employs the following software for fault tree development and quantification:

- FRANX, is used to add seismic initiators and hazard curves to the internal events model
- FTREX, generates cutsets from the fault trees produced in CAFTA
- ACUBE, is utilized for the SPSA quantification, since the SPSA introduces basic events, such as SSC fragilities, that significantly challenge the accuracy of the minimal cutset upper bound solution
- CAFTA, is used for SPSA fault tree development and review of results

15.6.2.7.3 Key Inputs and Assumptions

The key inputs are:

- Site-specific data is required as inputs for the seismic hazards PSA. Site-specific seismic hazard curves will be used in the future. The current analysis is based on data for a North American site.
- Plant-specific internal events models for at-power conditions.
- Characteristics of all PSA-modelled SSCs that are used for the seismic fragility analyses.

The following principal assumptions are used:

- Identical equipment fails at the simultaneous acceleration in case of a seismic event. Identical equipment is defined as being of the same type and located at the same elevation. This means that the failure events for identical pieces of equipment are 100% correlated. There is no credit taken for redundant systems of the same type.
- No recovery of offsite power or diesel generators is assumed. This is a severe restriction on mitigation capability.
- No repair of mechanical failures is assumed.
- Due to the high fragility of ceramic insulators in the switchyard, it is assumed that seismic events always result in a LOPP.
- It is assumed that valves and dampers that are failed seismically fail “as-is” (i.e., in the position they were in when the seismic event occurred).
- I&C components have a very high fragility compared to other components modelled in the PSA and can be excluded from the model without affecting the results.
- The components and systems that survive the earthquake have to function as designed to mitigate the accident. The probability of failure to function is estimated based on the internal events PSA model. The assumptions made in the internal event PSA are applicable for the seismic PSA also. For instance, the failure to run probability is calculated as a 24-hour mission time for all components unless otherwise stated or longer-term operation is needed to support safe-and-stable operation.
- Building structural failure causes failure of all equipment in the building. In general, failure of key buildings (such as the RB) yields failure that leads to loss of all mitigation.
- The failure of the containment leads directly to release.
- The random failure probability of a normally running system is negligible compared to the seismic failure of the system.
- Random failure probabilities of systems that survive the seismic event are calculated using the at-power PSA model, modified to reflect the available support systems. In these evaluations, the HEPs in the at-power PSA model are left unchanged.

15.6.2.7.4 Task Outputs and Preliminary Results

The SPSA CDF has been derived across a range of ground motion bins. The LRF is reported to be the same as CDF at this stage, with all core damage sequences treated as going straight to large release. The Level 2 analysis will be developed at a future point.

The following tasks have been completed:

- A seismic equipment list documenting the seismic capacity and fragility evaluation of SSCs
- SPSA model for at-power conditions
- Documentation of key assumptions and PSA modelling approach
- List of SSCs considered in the Level 1 PSA for seismic hazards and basis for any screening applied
- Fragility characterisation and the technical bases for them for each structure, system, and component
- Quantified probabilities of damage for the range of seismic hazards modelled in the Level 1 PSA
- Significant failure modes for SSCs and the location of each structure, system, and component
- Specific adaptations made in the Level 1 PSA model for internal IEs to account for the impact of the seismic events
- The methodology and procedures used to quantify seismic fragilities:
  - Seismic response analysis
  - Steps involved in screening
  - Review of design documents
  - Identification of critical failure modes for each structure, system, and component
  - Calculations of fragilities for each structure, system, and component

15.6.3 Level 2 Probabilistic Safety Assessment

An initial Level 2 PSA has been developed for the FPIE model to evaluate core damage sequences that have the potential to result in a release of radionuclides outside of the containment. The development tasks are discussed below.

15.6.3.1 Interface between Level 1 to Level 2 PSA

The characteristics of a core damage sequence that were used to inform the Level 2 PSA development include:

- RPV pressure at the time of core damage
- Timing of core damage
- Availability/failure of mitigating measures
- Containment failure
- Availability of containment isolation
- RPV rupture location

In order to capture these attributes, the Level 1 PSA sequences were binned into the following core damage classes. These are used to guide the creation of each Level 2 PSA Containment Event Tree (CET).

- Class I-M/I-L/I-OT - Core damage sequences occur with the RPV at low pressure and with containment intact. This class is broken down into three groups, medium LOCA, large LOCA and other transients. This ensures that all event characteristics, including event timing and available systems for mitigation are appropriately accounted for in the sequence progression.
- Class II - Core damage (core damage resulting from containment failure due to overpressure). Class II core damage often results from injection without containment decay heat removal. No Class II sequences have been identified.
- Class III - Core damage sequences that occur with the RPV at high pressure and that nominally have containment intact are Class III. No Class III sequences have been identified.
- Class IV/IV-L - Core damage with initial failure to scram. Those sequences where core damage occurs due to failure to inject negative reactivity using BIS (following successful ICS and other mitigation), experience late core damage whereas those with ICS failure result in early core damage. For all Class IV sequences (i.e., ATWS sequences), SA progression results in more severe RPV and containment conditions than those scenarios with successful reactivity control. The containment loading resulting from these scenarios is expected to exceed the containment capacity and gross failure of the containment is expected to occur.
- Class V - Core damage and an initial containment bypass. Containment bypass provides a radionuclide release path. Class V sequences result in large early releases.
- Class VR - Core damage occurs due to RPV ruptures in the lower or mid-vessel regions, triggering the containment vent in some cases.

This information is judged to be sufficient to characterise the plant state and serve as the basis for a set of CETs.

15.6.3.2 Containment Performance Analysis

The containment failure modes are analysed to identify the accident conditions that might lead to the containment failure. This analysis begins with a Level 2 accident progression literature survey and screening of SA phenomena.

Examples are shown below:

- NUREG/CR-4551 (Reference 15.6-33) (Grand Gulf and Peach Bottom analyses)
- Recommended sensitivity analyses for an Individual Plant Examination
- EPRI ALWR requirements document

A list of key phenomena where accident condition is considered is produced and then the evaluation methods for each phenomenon are studied.

The primary objective of an assessment of containment performance is to develop a realistic characterisation of the modes (mechanisms) of, and criteria for, containment leakage or failure under SA conditions. Design criteria for the containment are generally not adequate measures of capacity of the containment because of the safety factor built into such values. Actual values of the ultimate pressure capacity of the containment have sometimes been found to exceed design values by a factor of two to four. Further, containment design limits may not account for the harsh environmental conditions that can develop inside the containment during a SA, that often require consideration of entirely new failure modes.

Detailed information on the structural design of the containment and containment penetrations is required to generate a realistic assessment of containment performance limits. In the absence of this information at this stage in design development, informed judgements and assumptions are made in place of detailed analysis. FAP item PSR15.6 – 42 in APPENDIX B, captures the need to support the Level 2 PSA development with additional analysis.

The following containment failure modes have been considered to date in the Level 2 PSA:

- Hydrogen deflagration – hydrogen produced from cladding oxidation within the RPV may be released into containment during an accident. When reactor power is high and containment is not inerted, which is the case for a short period of time before and after refuelling outages, there is a risk of deflagration, resulting in containment failure and large release.
- Failure of containment isolation – this is modelled using the Level 1 PSA fault trees for containment isolation.
- Containment bypass – this occurs in sequences where there is a failure in RPV overpressure protection or containment overpressure protection, or where there is an un-isolated BOC, resulting in a large release.
- Direct containment heating – in Level 2 sequences where the RPV UPR system fails, there is fragmentation of the RPV and dispersion of debris throughout containment. The increased surface area of the debris results in direct containment heating, characterised by a rapid heat-up and pressurization of the containment atmosphere that leads to gross containment failure and a large release. This is modelled with the Level 1 logic for failure to open 2/3 UPR valves.
- Containment basemat melt-through - the corium shield is designed to prevent molten core concrete interaction in the event that corium relocates to the pedestal. A water pool is required to prevent the corium shield or the underlying basemat from failing due to high temperatures. In order to achieve this, water is released from an upstream tank into the pedestal by the pedestal water injection system. It is assumed that this system

will use a fusible plug valve to initiate the water injection and failure of this valve is modelled in the CET.

- Steam explosion in containment - if unquenched corium relocates into a pool of water a steam explosion can occur. This is modelled for sequences where corium from a failed RPV could fall into a water pool within the pedestal, made intentionally by pedestal water injection or unintentionally by a vessel rupture in the mid or lower vessel regions.
- Failure of containment venting - containment venting is used to filter aerosol-based radionuclides which are discharged from containment and into the equipment pool via the containment vent. Failure to filter and failure to relieve pressure are both considered in the CETs, using expert judgement for filtration effectiveness and modelling of the containment vent system from the Level 1 PSA.
- Containment overpressure – this occurs when containment pressure exceeds its ultimate failure pressures. No containment performance assessment is yet available and so assumptions have been made regarding which events result in containment overpressure, including all core damage events due to ATWS.

15.6.3.3 Accident Progression Analysis and Development of the Containment Event Trees

The engineered safety features and the operator actions which can influence the progression of SAs, the containment response, and the transport of radioactive materials are identified and highlighted. The current Level 2 PSA iteration contains a number of conservative assumptions commensurate with the design development. Additional supporting analysis will be undertaken going forward as more detailed design information becomes available. The safety features and operator actions will be identified in line with the plant and site-specific severe accident guidelines (that will be developed prior to operation), available plant design information, and design requirements for the SA conditions. No additional operator actions have yet been identified as part of the Level 2 PSA.

Further consideration of the SA phenomena and analysis is discussed in PSR Subchapter 15.5 Section 15.5.6.

15.6.3.3.1 Accident Progression Analysis

- Selection of Accident Sequence and Analysis Condition

  There are many possible scenarios that lead to core damage. Therefore, some cases are selected as the representative cases through the grouping process. The selection of IEs and availability of mitigation systems are determined based on the characteristics of plant responses and effect on radionuclide releases, which are identical to those in the core damage class identification process.

- Accident Progression Analysis

  Accident progression analyses for each representative case will be performed in order to obtain the data which is necessary for the development of CETs, such as plant thermal-hydraulic behaviour, chronology of accident progression (the timing of the core damage and the containment failure), and containment loads from SA phenomena. Accident progression analyses will include both cases in which mitigation systems fail or succeed.

  Limited analysis has been performed to date, with the bulk of the CET development based on expert judgment and assumptions. Going forward, MAAP (Reference 15.6-60) will be used for the accident progression analysis in the Level 2 PSA of BWRX-300. This analysis will include models for the important accident phenomena that might occur in the RPV, in the primary containment vessel, and in the RB. The consequence analysis software MAAP calculates the progression of the postulated accident sequence, including the deposition of the radionuclides, from IEs to either a safe, stable state or to an impaired containment condition (due to overpressure or overtemperature). The software also calculates the amount of radionuclides released to the environment.

Chronological results of accident progression analyses will be used as indication of available time for operator actions such as the coolant injection after the core damage and recovery actions.

- Analysis on Occurrence Probability of Physical Phenomena

  Occurrence probabilities of physical phenomena such as in-vessel/ex-vessel steam explosion, Direct Containment Heating and Molten Core Concrete Interaction are evaluated. Each branch probability is estimated using expert judgment, Level 1 PSA fault trees, component reliabilities and analysis performed for similar plants. As the design develops, specific containment performance analysis and thermal hydraulic analysis will be undertaken.

- Accident Sequence Analysis (Development of Containment Event Tree)

  Containment event trees are developed for each core damage class. A generic containment event tree is initially used and then tailored for each core damage state to ensure that all appropriate conditions are assessed given the conditions at the time of core damage.

  The top events in a containment event tree address the events and physical processes that govern accident chronology, plant response to beyond design basis conditions, relevant challenges to barriers to radioactive material release and the eventual magnitude of the release of radioactive material to the environment. These generally reflect the containment failure modes discussed in Section 15.6.3.2 above. Other top events include probability of the containment being inerted, decay heat removal with ICS and consideration of the water level in containment.

  The containment event tree structure is chronologically correct, accounts for interdependencies among events and/or phenomena, and reflects an appropriate level of detail to satisfy the objectives of the Level 2 PSA. This will be reassessed as the Level 2 PSA develops.

  The effect of the environmental conditions resulting from a SA on the survivability of components and systems credited within the Level 2 PSA model are also assessed and appropriately accounted for. Environmental conditions may include temperature, pressure, humidity, and radiation conditions, as well as effects derived from energetic events (e.g., short-term temperature and pressure spikes or impulse loadings from detonations or steam explosions).

  Potential adverse effects of SA management actions are also considered as part of the event tree logic. For instance, injection of water into a degraded core may be able to arrest the progression of a SA. However, there is also the potential for energetic fuel coolant interaction, fuel shattering and additional releases of steam, hydrogen, and radioactive material. Dependency of SA phenomena on success/failure of mitigation systems are modelled.

  By linking the fault trees to containment event trees, dependencies regarding basic events including component, support systems, operator action and success logic (“NOT” logic) are captured in the analysis. In addition, the containment event trees are connected to all relevant Level 1 core damage sequences. This enables treatment of dependency between the Level 1 PSA and the Level 2 PSA. System fault trees in the Level 2 PSA are developed in line with the steps for the Level 1 PSA discussed above.

Mitigating measures (i.e., equipment and operator actions) and their failures are addressed via fault trees. This interface is addressed inherently by coupling the Level 1 model with the Level 2 model so that any basic events relevant to both core damage and radionuclide release propagate to both levels of the PSA model. To the extent that is possible and appropriate, the same dependency modelling and basic events are used in both models.

Currently, the Level 2 PSA assesses the following release classes and results are presented for these metrics:

- Large early release, inerted containment
- Large late release, inerted containment
- Filtered early release, inerted containment
- Filtered late release, inerted containment
- Large early release, de-inerted containment
- Large late release, de-inerted containment

For release timing, a release is considered early if it occurs within 24 hours following core damage and late if it occurs beyond 24 hours following core damage.

Going forward, a full set of release categories will be defined in conjunction with the SA Analysis and Level 3 PSA development, with source term analysis being undertaken for each release category. The attributes used to define the release categories will take account of key characteristics that influence the release of radioactive material from containment. Characteristics of such events include:

- The mode and time of failure of the containment
- The cooling mechanisms of the molten core material
- The retention mechanisms for radioactive material

If this process generates a very large number of release categories, these will be further grouped into a manageable set that can be used in the source term analysis.

The end states of the containment event tree will be grouped into the specified release categories. As this involves the grouping of typically thousands of end states of the containment event tree into a small number of release categories, a systematic process will be applied to this grouping process. The frequency of the release categories will be calculated by summing the frequencies of all the end states of the containment event tree that are assigned to the group.

15.6.3.4 Model Integration and Quantification

The Level 2 PSA model is integrated with the Level 1 PSA model. The Level 1 accident sequences are placed under “collector gates” that group core damage sequences into classes. The Level 2 ETs are constructed with the entry branch name identical to the applicable Level 1 Core Damage class collector gate. Functional node branches are given names identical to those in the functional fault tree file. When the event trees are converted into fault tree logic (creating accident sequence logic) and merged with functional fault tree logic, an integrated, quantifiable fault tree is developed. The fault tree is quantified using CAFTA and PRAQuant model development codes.

In addition, FTREX is used as the quantification/cutset generation engine and system is used to develop importance measures for systems, components, and HFEs.

The cutsets are quantified at a truncation of 1E^{-15}/yr and examined to ensure there is <5% top event frequency drop if the truncation limit is set to 1E^{-14}/yr. This provides evidence that no risk-significant sequences have been truncated.

15.6.4 Uncertainty And Sensitivity Analysis

The uncertainty and sensitivity analysis performed for the BWRX-300 PSA model provides the uncertainty distribution for the overall risk calculated previously. The sensitivity analysis evaluates the sensitivity of the results to key model assumptions. The combined results of the two analyses describe the overall uncertainty of the PSA and identify those PSA attributes significantly affecting the PSA results.

The uncertainty results presenting the lower/upper bounds and the spread of the mean value of the risk are considered a good representation of the aleatory uncertainties of the model, which are related to random processes. The sensitivity cases represent the epistemic (modelling) uncertainties, which are related to deficiencies in knowledge. Therefore, the sensitivity study results add valuable insights for the users of PSA results, future PSA model updates, and the identification of potential model deficiencies. Various sensitivity analyses are conducted on the BWRX-300 PSA at-power, fire, flood, high wind, seismic, and shutdown models. Uncertainty analyses are performed on the Level 1 and Level 2 baseline internal events PSA models. The intent of these analyses is to evaluate the effects to the PSA models and to provide risk insights. Sensitivities and uncertainties are identified from the following sources:

- Support for key assumptions
- Identified by system/PSA engineer

Whereas sensitivity analysis is used to measure the extent to which results change if alternative models, hypotheses or values of input parameters were selected (and thus provides an evaluation of uncertainty in respect of a particular issue or a particular group of related issues at a time), uncertainty analysis examines a range of alternative models or parameter values, assigns each model or value a probability and generates a distribution of the results, within which the baseline results represent one possible outcome. Each result within the full distribution is accompanied by a (subjective) probability representing the degree of belief in that result. Cumulative probability levels for the results can be calculated (e.g., the 5th, 50th and 95th percentiles represent 5%, 50% and 95% probabilities, respectively, and the ‘true’ result is below the respective level for which each of these probabilities is stated).

The methodology for conducting the sensitivity and uncertainty analysis was conducted in three phases: (1) selection/identification, (2) implementation/analyses and (3) results/benchmarking. The first step was to evaluate the importance of the sensitivity itself. In some cases, sensitivities were identified, but upon further evaluation were discarded due to inherent model conservatisms or were delayed pending more detailed engineering.

15.6.4.1 Identification and Characterisation of Uncertainties

The following guidance was used to identify any additional modelling uncertainties:

- EPRI-1009652, "Guideline for the Treatment of Uncertainty in Risk-Informed Applications: Technical Basis Document,” (Reference 15.6-61)
- EPRI-1013491, "Guideline for the Treatment of Uncertainty in Risk-Informed Applications: Applications Guide” (Reference 15.6-62)
- EPRI-1016737, "Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments” (Reference 15.6-63)
- NUREG-1855, "Guidance on the Treatment of Uncertainties Associated with PSAs in Risk-Informed Decision Making - Main Report” (Reference 15.6-64)
- EPRI-1026511, “Practical Guidance on the Use of Probabilistic Risk Assessment in Risk- Informed Applications with a Focus on the Treatment of Uncertainty,” (Reference 15.6-65)

The above provide examples of generic uncertainties for each of the PSA tasks, that may or may not be applicable to the BWRX-300. The identified generic uncertainties are reviewed for applicability to the BWRX-300 and assessed if applicable. In addition, the PSA assumptions are reviewed for key assumptions affecting the results. Each key assumption is then assessed qualitatively or quantitatively through sensitivity analysis. When a quantitative assessment is not possible, or if the quantitative assessment is not valuable (i.e., the analysis is trivial), then a qualitative assessment is performed.

EPRI 1026511 (Reference 15.6-65) provides a framework for addressing uncertainty in a SPSA. Table C-1 of that report lists various sources of model uncertainty and possible resolutions of these issues. It can be used to identify and characterise any uncertainty (generic, plant-specific modelling and completeness uncertainty).

Key (risk-significant) assumptions are judged based on guidance from the ASME standard. Factors that are considered include a determination if the assumption is conservative or optimistic and an investigation into the risk importance measures (i.e., Fussell-Vesely importance and RAW). If the importance of the assumption is not able to be confirmed based on a calculated importance measure, then the risk impact from the assumption is confirmed by sensitivity analysis. The impact of all significant assumptions is assessed by performing sensitivity studies that apply different plausible assumptions. If assumptions affect the same aspects of the PSA model, then sensitivities are performed concurrently.

The focus of the analysis is epistemic uncertainty (i.e., uncertainties in the formulation of the PSA model). The different types of epistemic uncertainty are:

- Parameter uncertainty
- Model uncertainty
- Completeness uncertainty

These are addressed through the uncertainty and sensitivity analysis discussed below.

15.6.4.2 Level 1 PSA Analysis

15.6.4.2.1 Parametric Uncertainty Analysis

For parametric uncertainty, the first step is to identify the range of values of uncertain parameters. Each value within the range of values that the uncertain parameter can take on is associated with a probability, thereby creating a probability density function or probability distribution.

UNCERT is used for parametric (statistical) uncertainty analysis, which involves the propagation of uncertainties through the PSA. UNCERT was developed by EPRI and is a program to perform the uncertainty analysis using a Monte Carlo method. UNCERT generates the random inputs based on the user specification, calculates all intermediate values such as component failure probabilities, and calculates the top event value from the cutsets. In addition, the state of knowledge correlation per parameter uncertainty is naturally considered as described in the user’s manual of UNCERT. This is handled by the use of type codes so that basic events that share a failure rate will be tied to the same type code.

A mean CDF value is generated from this analysis together with an uncertainty distribution, with the 5th percentile, median and 95th percentile values also being reported in the results.

15.6.4.2.2 Sensitivity Studies

Major model assumptions in the BWRX-300 system notebooks and any changes made to the BWRX-300 PSA models as a part of the update process are reviewed to identify the candidate sensitivity cases. Some of the important assumptions are related to the uncertainties caused by the lack of thermal-hydraulic analysis supporting PSA modelling and should be investigated in this task. The overall effect of the maintenance unavailability, the CCF probabilities, and human reliability analysis probabilities are included in the analysis. To date, the Level 1 internal events PSA sensitivity studies include:

- All HEPs set to their 5th percentile value (the use of zero-value HEPs is also deemed acceptable)
- All HEPs set to their 95th percentile value
- All CCF probabilities set to their 5th percentile value (the use of zero-value CCF probabilities is also deemed acceptable)
- All CCF probabilities set to their 95th percentile value
- All maintenance terms at zero (zero-maintenance model)
- ICS passive reliability
- HVS impact on control building equipment
- Safety Class 3 Software CCF probability

For the full power model, the following additional studies were conducted:

- Additional success path for ATWS sequence
- RPV rupture axial location distribution

For the LPSD model the following additional studies were conducted:

- (LOCA frequency for LPSD operation
- FLEX/EME injection in Plant Operating State (POS) 3, 4 and 5
- POS duration
- Maintenance event for CRD system

The SFP PSA also performed sensitivity studies to look at the impact of a potential design change and the use of FLEX for refilling the pool.

15.6.4.2.3 Hazards Uncertainty and Sensitivity Analysis

For the various hazards considered as part of PSA, uncertainties have been reviewed and characterised. This has included identification and review of generic, modelling and completeness uncertainties throughout the various stages of the PSA development. As part of the uncertainty characterisation, the following aspects have been evaluated: part of the model affected; plant specific approach taken; assumptions made; impact or model and characterisation assessment.

Being the design phase, the level of maturity across the different forms of hazard being evaluated varies and this directly impacts the extent of uncertainty and sensitivity analysis performed at this stage. Some examples of analysis performed across the four main hazards considered at this stage are as follows.

Fire PSA key uncertainties and related assumptions for all fire PSA elements are documented; this includes performance of parametric uncertainty. Just focusing on quantification related uncertainties and assumptions, the key sources of uncertainty relate to some of the conservative treatments applied which include use of assumed cable routing exclusively for the development of the target damage sets; full room burnups modelled for almost all scenarios; no delay time for target damage and no credit for fire detection and suppression.

For the SPSA, following the review of the generic, modelling and completeness uncertainties, a number of key sources of uncertainty were identified. One of the more significant examples involves modelling of the seismic failure of the polar crane which currently leads directly to core damage and containment bypass due to SSCs from the damaged crane dropping to the RB refuelling floor. Due to the significance of the consequence, a relatively high seismic capacity target is modelled for the crane fragility group. However, no structural analysis of the consequences of crane damage has been performed at this stage, therefore the SPSA modelling of the crane fragility group introduces a key source of uncertainty. A number of sensitivities have been performed to evaluate impact on risk from different modelling approaches, changes in input or to attempt to characterise uncertainties. As an example, a sensitivity has been performed to evaluate the benefit of implementation of an anticipatory automatic seismic trip system.

Following review of uncertainties related to the high wind PSA, one of the key modelling uncertainties was identified to be the gradual approach applied to scale missile damage probabilities across a suitable range of wind speed bins for the tornado and hurricane models. Generally, lower wind speed bins are credited with lower missile impact probabilities based on engineering judgement, while higher wind spend bins retain the default probability of 1.0. A sensitivity evaluation revealed the significance of these missile impact fragilities values to the risk. An example of a completeness uncertainty identified, relates to the need to consider additional wind loading due to the combination of wind and rain.

Some areas of the hazard uncertainty and sensitivity analysis still need to be developed further. Parametric uncertainty analysis has not been performed at this stage and will be developed in future PSA updates.

15.6.4.3 Level 2 Uncertainty and Sensitivity Analysis

Uncertainty arises in a Level 2 PSA analysis as a result of several factors, including:

- Incompleteness uncertainty. The overall aim of a Level 2 PSA is to assess the possible scenarios (sequences of events) that can lead to releases of radionuclides. However, there is no guarantee that this process can ever be complete and that all possible scenarios have been identified and properly assessed. This potential lack of completeness introduces an uncertainty in the results and conclusions of the analysis that is difficult to assess or quantify. It is not possible to address this type of uncertainty explicitly. However, peer review can reduce this type of uncertainty.

- Loss of detail due to aggregation. Grouping accident sequences or cutsets from the Level 1 PSA into PDSs for input into the Level 2 PSA for practical reasons also introduces uncertainties due to the resulting loss of some modelling detail. Further, the process of ‘binning’ (or grouping) accident sequences introduces uncertainty through the possibility that the attributes used by the analyst to group ‘similar’ accident sequences are incomplete.

- Modelling uncertainty. This arises due to a lack of complete knowledge concerning the appropriateness of the methods, models, assumptions, and approximations used in the individual analysis tasks that support a Level 2 PSA. Modelling uncertainties are addressed in the sensitivity analysis.

- Parameter uncertainty. This arises due to the uncertainties associated with the values of the fundamental parameters used in the quantification of the Level 2 PSA, such as equipment failure rates and IE sequences.

At this stage in development, the Level 2 PSA uncertainty analysis has been performed qualitatively, assessing the level of uncertainty present in the input parameters used to perform the Level 2 PSA quantification. The scope of this assessment has been limited to the parameters used in the CET branch point quantification. As the Level 2 PSA develops and is supported by further analysis, many of these uncertainties will diminish.

Sensitivity analysis was undertaken by varying the baseline value of a number of parameters by an appropriate factor in order to bound any potential uncertainties that may exist. These parameters, such as the duration for which containment is de-inerted, the failure probability of the pedestal water injection system, or the probability of steam explosion are all based on best estimate assumptions at the present stage in design development. This analysis will be further developed in future, with additional analysis conducted to investigate the propagation of uncertainties from the Level 1 PSA.

15.6.4.3.1 Task Outputs and Preliminary Results

The following are key task outputs:

- Risk-informed BWRX-300 design changes
- Key insights and assumptions confirmed by sensitivity studies

15.6.5 Level 3 Probabilistic Safety Analysis

Development of the Level 3 PSA has not yet been undertaken. The requirement to develop a full scope Level 3 PSA has been captured as FAP item PSR15.6-40, see APPENDIX B.

NEDC-34357P, “BWRX-300 UK GDA Safety Case Manual Specification”, (Reference 15.6-66), was produced during GDA Step 2. This specification outlines the requirements for a SCM for the deployment of the BWRX-300 baseline design in the UK, which the future phases of the project need to consider. Within this specification it sets out the activities that will need to be undertaken in order to perform a full scope Level 3 PSA.

15.6.6 Results Of the Level 1 Probabilistic Safety Assessment

The results of the PSA are considered to be order of magnitude estimates at this stage, given the uncertainties that exist in each step of the PSA development process as documented in each of the supporting analyses. The PSA has been performed using the design information that is available at the time of the assessment and this has resulted in conservative assumptions being made in the absence of further information. This is particularly true on the case of hazards assessments where detailed design information such as cable routing is not yet available. Therefore, the various assessments each contain differing degrees of conservatism and uncertainty, which limits the usefulness of combining all the results to obtain an overall core/fuel damage value. Nevertheless, this has been done in order to enable an early comparison with the plant safety goal. These uncertainties and conservatisms will continue to diminish in each iteration of the PSA.

PSR Subchapter 15.9 Table 15.9-9 shows the PSA CDF results to date. The PSA model was quantified by using input from each PSA technical element to produce cutsets describing core damage (or fuel damage in the SFP PSA) sequences for the BWRX-300. The overall calculated risk is very low compared to historical CDF values calculated for existing plants. There is significant margin to the safety goals typically applied by IAEA member states as documented in IAEA-TECDOC-1874 (Reference 15.6-13).

The total plant CDF, including FDF from the spent fuel pool contribution, is 8.73E-07 /yr. Almost 94% of this is from the seismic analysis. This early version of the seismic analysis is known to be conservative, due to the limitations given the early phase of the design.

The percentage contributions to the combined core and fuel damage from the other elements of the PSA are as follows:

- Internal fire events – 1.7%
- Spent fuel pool events – 1.4%
- FPIE – 1.2%
- Internal flooding events – 0.6%
- Wind events – 0.5%
- Fuel damage from heavy load movements (*core damage included in LPSD result) – 0.5%
- LPSD – 0.1%

Concern that small changes can lead to large differences in plant effects (i.e., cliff-edge effects) are largely ameliorated by the demonstrated margin between CDF and the plant safety goal. Within the PSA accident sequence and success criteria analysis, no cliff edge effects were discovered where plant parameters approach critical thresholds where accident sequences are expected to follow a significantly more severe pathway. However, uncertainty in these analyses will be formally explored in more detail in future PSA work.

15.6.6.1 Full Power Internal Events Results

The CDF has been estimated as 1.06E-08/yr for FPIE PSA. The core damage frequency relating to the internal events level is relatively low compared to historic BWR core damage frequencies. This is because many of the significant contributors to risk have been designed out for the BWRX. As a result, the overall risk is low, and the most significant contributors are not those commonly seen. At this stage in the development, this is still seen as an order of magnitude estimate given the level of uncertainties.

The top initiating event contributing to the internal events at-power risk is an excessive LOCA/reactor vessel rupture. These failures are un-isolable and there is limited mitigation available should such an event occur. Therefore, despite a low initiating event frequency, the risk is relatively high. The top two cutsets relate to this event (split between rupture in lower vessel and mid vessel) and together contribute almost 50% of the FPIE CDF. The initiating event frequency has been refined from generic data for the BWRX, but further refinement may be possible as the design develops, especially regarding conditional break location probabilities.

Un-isolable medium LOCAs contribute 15% to the CDF, when combined with the failure of the CRD injection flow. Again, there is potential to further refine the LOCA frequencies as the design develops, especially with regards to the way the frequency is apportioned between isolable and non-isolable frequencies.

ATWS sequencies with Loss of Preferred power make up nearly 18% of the CDF. The modeling for these sequences will be an area of focus in the next PSA iteration, especially with regards to reducing the conservatisms relating to the success criteria.

The uncertainty result in Table 15.6- 6 shows that the mean is towards the higher end of the distribution and even with the use of the 95th percentile results, the margin to the plant safety goal would not be significantly eroded.

15.6.6.2 Low Power and Shutdown Internal Events Results

The CDF is calculated to be 1.2E-09/yr.

As expected, the contribution to CDF from the LPSD internal events is small in comparison to the full power risk (11% compared to the FPIE results). The top contributing initiating events all relate to loss of both SDC and CRD injection. This includes loss of offsite power, as both the SDC and CRD injection are dependent on the diesel generators, resulting in high importance for the diesels. Loss of the CRD purge water pump or loss of the CST, also lead to loss of both SDC and CRD injection, thus having a severe impact on the plant's ability for mitigation. This leads to core damage when combined with failure of ICS, dominated by head vent line isolation failure.

The uncertainty distribution in Table 15.6- 7 shows some discrepancy between the point estimate and the mean value. This is due to the importance of the maintenance events of the diesel generators and the shared uncertainty distribution.

15.6.6.3 Spent Fuel Pool Results

The FDF is calculated to be 1.25E-08/yr. The SFP analysis is an initial analysis, and the results are known to be conservative relative to the latest design (which this analysis helped to inform). This is discussed further in Section 15.6.8. The design change will also impact the operator actions, which are also significant contributors for the SFP risk.

15.6.6.4 Hazards Results

The hazards analyses are shown to be some of largest contributors to CDF. As mentioned above, a number of conservative assumptions have had to be made at this stage in order to overcome limitations in the availability of detailed design information. This is particularly prevalent for hazards PSA and as the analyses mature and are refined, the level of uncertainty will be reduced.

The internal fire PSA contribution to CDF was estimated to be 1.50E-08/yr. It was found the majority of the contributions arise from fires that produce a general transient, the next largest contribution coming from loss of FW induced initiators. The single top contributing fire scenario was following a fire in the dewatering pump room (PAU 3177), where the fire target damage set resulted in a loss of FW and a loss of DL4a scram and ICS actuation signals. The internal flood PSA contribution to CDF was reported to be 5.26E-09/yr. It was shown floods initiating in the turbine building 1st floor area room (PAU 2170) aid the main steam and FW piping room (PAU 1670) where some of the top contributors to risk. At this stage the external hazard analyses have not yet been developed for a specific site. Whilst the analyses presented are based on hazard characterisation performed for North America; they are indicative of how the external hazards PSA will be developed once more information on site location is available. As such, there is a high level of uncertainty associated with these results. With this in mind, the seismic PSA contribution to CDF was estimated to be 8.20E-07/yr. Whilst it may be premature to evaluate the combined CDF profile of the plant at this stage, the seismic events are shown to make a dominant contribution. The seismic PSA results reveal that the majority of contributions to the SPSA risk arise from seismic damage of RB/containment, which is modelled to lead directly to core damage. The second significant contributor is LOPP, which is modelled to occur for all earthquakes modelled by the seismic PSA. The high wind events contribution to CDF was estimated to be 4.12E-09/yr. The percentage contributions from the three main categories of high wind hazard considered were shown to be 55% from hurricane, 31% tornado and 14% straight wind.

15.6.7 Results of the Level 2 Probabilistic Safety Assessment

PSR Subchapter 15.9 Table 15.9-10 shows the PSA LRF results to date.

The full scope Level 2 PSA has not yet been completed. Level 2 PSA has only been undertaken for FPIE, wind and internal fire PSA. Therefore, the plant LRF cannot be accurately reported and compared to the safety goal. However, if CDF values are substituted in place of LRF values which are yet to be assessed, in order to calculate a full plant LRF, the IAEA safety goal of 10E-6/yr is met, although the plant goal of 1E-7/yr is exceeded. This is dominated by the seismic risk, for which a Level 2 PSA has not yet been conducted.

The Level 2 PSA is currently based on conservative assumptions, given the limited availability of supporting containment analysis and severe accident analysis at this time.

15.6.7.1 FPIE PSA results

The large release frequency for the FPIE PSA is calculated to be 2.37E-09. This makes up 20% of the total release frequency for FPIEs, with the remaining 80% being filtered releases. No small releases were identified.

Vessel rupture events contribute 38% of the large release frequency. ATWS sequences go directly to large release and as such these sequences also contribute a significant proportion of the LRF, (36%). Medium LOCA and steam line and FW BOC events also contribute significantly.

15.6.7.2 Hazards Results

As mentioned above, the Level 2 PSA has not yet been developed for all the hazard analyses and in these instances core damage/fuel damage sequences have been conservatively assumed to go straight to large release. For the instances where Level 2 PSA has been developed for hazards, these results are described below.

The internal fire PSA contribution to LRF was calculated to be 2.67E-09/yr, with general transient and loss of FW induced initiators being the main contributors. The single top contributing fire scenario was following a fire in the DL4a room (PAU 4176), where damage to the target set resulted in loss of DL4a scram and ICS actuation signals. The high wind events contribution to LRF was shown to be 7.64E-10/yr. The percentage contributions from the three main categories of high wind hazard considered were estimated to be 92% from tornado, 6% hurricane and 1% straight wind.

15.6.8 Probabilistic Safety Assessment Insights and Applications

The development of the BWRX-300 PSA is an iterative process as more detailed design information becomes available and more analyses are performed. As such, the current PSA results do not present the full site risk from a full scope PSA. They do however show the order of magnitude of expected risk, which can be seen to be very low compared to traditional BWR plants. At this stage in design development, the most important use of the PSA is to provide risk insights to inform design.

The PSA feeds into the integrated design engineering process depicted in Figure 15.6- 1. This is described in 006N3139 (Reference 15.6-12) and explained in more detail in NEDC-34158P, “BWRX-300 UK GDA PSA Strategy Report,” (Reference 15.6-44).

Most significantly, following early analysis, the PSA results informed the key decision for an alternative RPV depressurization mechanism in addition to the ICS to be incorporated into the design. This has resulted in the requirement for the ultimate pressure regulation system, which is currently under design development.

Other aspects of the design that have been significantly informed by the PSA are:

- Addition/sizing of filtered containment vent
- Supporting the need for a boration mechanism
- Sizing/operation of CRD injection to provide makeup
- Seismic capacity requirements for select equipment
- Spatial separation in select areas for fire considerations
- Shutdown nuclear safety strategies
- Potential for seismic anticipatory trip
- Development of FLEX/EME functions
- Precluding need for new RPV nozzle to accommodate boration

The current set of results, including importances and sensitivity studies offer insights into the risk profile of the design, and where to prioritise work to reduce uncertainties. Some of the main findings of the current set of results are presented below. More information is provided in the PSA Summary Report, 008N9751 (Reference 15.6-10).

15.6.8.1 FPIE Level 1 PSA

The following lists the key risk insights from the FPIE Level 1 PSA model results:

- Reactor vessel rupture is currently a significant contributor to risk. However, there is significant uncertainty in the frequency calculation and conditional break location probabilities. Sensitivity studies showed the CDF to be sensitive to assumptions made regarding the rupture location.
- The non-isolable LOCA frequencies need refining as more detailed design information becomes available, given the significance of these events. In addition, the discrepancy between the definition of LOCA size in the generic data and that used to define success criteria needs to be resolved to ensure mitigation is accurately captured, see FAP item PSR15.6 – 52 in Appendix B.
- ATWS sequences are important contributors to risk. The CCF of the control rods failing to insert acts as a floor value to the ATWS frequency. This CCF may be refined further as the control rod drive system design develops. The success criteria for these sequences are currently based on conservative assumptions and further thermal hydraulic analysis will be undertaken to refine the modelling of these sequences. This

may also enable blowdown through the UPR system to be credited as mitigation, which is not currently the case, see FAP item PSR15.6 – 57 in Appendix B.

- Common cause software failure is important to the overall risk of the plant. Sensitivity studies showed significant sensitivity to increases in the failure probability for Safety Class 3 software, which is the dominant failure mode of CRD injection and therefore impacts non-isolable large and medium LOCAs. The I&C modelling will be refined as the design evolves, with learning from the PSA informing the design development, see FAP item PSR15.6 – 59 in Appendix B.

- The importance results (high RAW with a low Fussell-Vesely contribution to CDF) show that the reliability of the ICS is key to the overall risk of the plant. A sensitivity on the inclusion of passive reliability for this system shows that the CDF is sensitive to the introduction of this parameter, particularly affecting transient events. A plant specific passive reliability assessment of the ICS has been included as FAP item PSR15.6 – 48 in Appendix B.

- The current model assumes that CRD is the only high-pressure injection source. Currently, the use of low-pressure injection (via FLEX) is not credited in the Level 1 FPIE PSA. While this function is not of great importance now, further model refinements may result in it being so, and enabling a function to refill the CRD suction source could be explored.

- Venting of both the RPV and containment are credited in the PSA model, but no final design has yet been decided. Incorporating credit for these systems is a benefit for design optioneering and can be used to help inform how best to risk-inform the specific designs. The current PSA model includes assumed design (e.g., capability and setpoint for RPV pressure relief and venting) on which the success criteria are based. Since the sensitivity of these systems is small based on the current results, it is important to track the design progress to avoid drastic change of risk impact of these systems, see FAP item PSR15.6 – 56 in Appendix B.

Design optioneering with input from the PSA team will continue as the BWRX design development matures.

15.6.8.2 LPSD Level 1 PSA

Dependent failure of SDC and CRD injection events dominate the LPSD risk. CRD injection shares CRD purge water supply line and the CST with SDC. Therefore, it may be possible to lower the risk if this dependency could be removed in the design.

The ICS is a very reliable system due to the three redundant trains. However, in LPSD operation, head vent isolation is an additional failure mode (noting the ICS can only be used in those modes for which the reactor can be pressurised). When a boil-off event occurs and ICS is used for decay heat removal, the head vent line needs to stay open for a while to allow the inventory to boil down to the ICS steam inlets and then needs to be closed in order to allow the reactor vessel to pressurise. Failure of the head vent isolation valve to close is the dominant failure mode of ICS in shutdown operation modes since it is not divisionally redundant in contrast to the other ICS components. Therefore, improving the reliability of the isolation would be beneficial to risk.

15.6.8.3 Hazards Level 1 PSA

With the hazards analyses being in the early stages of development and the high level of uncertainty involved, the insights highlight more the key areas of uncertainty and where development should be focused in order to achieve more refined results. These aspects are discussed further in the Uncertainty and Sensitivity Analysis Section 15.6.4. Instances where meaningful insights could be ascertained are described below.

15.6.8.3.1 Internal Flooding

- The top cutset contributor to CDF is from a scenario whereby the flood initiates in the turbine building 1st floor area room (PAU 2170), greater than 50 gpm flood leak rate, with the flood source being the liquid waste management system (K10) piping and components. It has a high flood frequency of 9.39E-3/year, with most of the flood frequency coming from tank, manual valve, motor driven pump and air operated valve ruptures. A possible way to mitigate the risk is to prevent a "Loss of Condenser Heat Sink”.
- Initiator by protecting the FW and plant cooling water targets in this flood scenario. That is, a flood in PAU 2170 should be prevented from reaching the critical failure height of the condensate and FW system (N21) and plant cooling water system (P40) flood susceptible components.
- Based on the second and sixth top cutset contributors, minimizing piping and components for the control rod drive (G12) and LWM (K10) systems in the main steam and FW piping room (PAU 1670) will reduce the risk contribution of these cutsets. The three trains (A, B, C) of C20 high RPV pressure sensors/transmitters are assumed to be located near the steam lines in PAU 1670. This assumption is driving up the CDF contribution of cutset #2 & #6 by causing the ICS condensate return valve to fail to open (via DL 2 or DL4a signal) due to flood induced failure of C20 High Pressure Transmitters. The three trains (A, B, C) of C20 high RPV pressure sensors/transmitters could be installed in separate locations in such a way as to prevent an internal flood from simultaneously failing all three instruments.

15.6.8.3.2 High Winds - Straight Wind

The total straight wind CDF is 5.57E-10/yr, with wind speed bins 1 through 4, from 117 km/h to 186.5 km/h presenting about 87% of straight wind risk.

The dominant straight wind CDF contributors are CCF of all ICS reactor isolation condensate return valves or CCF of all ICS reactor isolation steam supply valves, resulting in isolation condenser failure to remove decay heat.

15.6.8.3.3 High Winds - Tornado

The total Tornado CDF is 1.29E-09/yr, with wind speed bins 1 through 7, from 172 km/h to 292 km/h presenting about 82% of tornado CDF risk. When considering individual bins, wind speed bins 3 and 4, ranging between 206 km/h and 241 km/h, provide a large risk contribution to CDF.

The dominant tornado CDF contributor is Defense Line 3 common cause software failure.

15.6.8.3.4 High Winds - Hurricane

The total hurricane CDF is 2.27E-09/yr, with wind speed bins 1 through 3, from 119 km/h to 160 km/h present about 87% of hurricane CDF risk.

The dominant hurricane CDF contributors are CCF of all ICS reactor isolation condensate return valves or CCF of all ICS reactor isolation steam supply valves, resulting in isolation condenser failure to remove decay heat.

15.6.8.3.5 Seismic

The SPSA results reveal that the majority contributions to the SPSA results arise from seismic damage of RB/Containment, which is modelled to lead directly to core damage and containment bypass (plant damage state CD_V). The second significant contributor is a LOPP, which is modelled to occur for all earthquakes modelled by the SPSA. Less significant contributors include seismic damage of the bridge crane and RPV support structure.

The SPSA has been used to set seismic capacity requirements for risk significant SSCs and these have been used in the analyses. Utility requirements document generic fragilities are used for non-risk significant SSCs. The development of plant-specific fragilities has the potential to significantly increase or decrease the SPSA CDF results.

Seismic failure of the polar crane is modelled to cause core damage and containment bypass due to SSCs from the damaged crane dropping to the RB refuelling floor. Due to the significance of this consequence, a relatively high seismic capacity target is modelled for the CRANE fragility group, Am = 8.4g. However, no structural analysis of the consequences of crane damage has been performed. Therefore, the SPSA modelling of the CRANE fragility group introduces a key source of uncertainty and is an area for further work.

Sensitivity studies have shown that crediting an anticipatory automatic seismic trip system for the BWRX-300 design reduces the base case CDF by approximately 10% so this is something for future consideration.

15.6.8.4 Spent Fuel Pool

The spent fuel pool results highlighted a single point vulnerability in the SFP make up path, with a single MOV failing to open resulting in failure to inject water from both the CST and Fire Protection system. As a result, a design modification was proposed to add an air operated valve in parallel with the original MOV to add redundancy and diversity to this make up path. The design of the injection paths has since been developed, with redundant make up paths, thereby removing the need for the additional valve. The latest design has not been incorporated into the SFP model, but the original calculations associated with the design proposal showed removing the single point vulnerability would reduce the calculated fuel damage frequency by almost a factor of 3.

15.6.8.5 FPIE Level 2 PSA

The current results are largely based on conservative assumptions and expert judgement. The results highlight the areas for which additional analysis is priority and also which assumptions need to be validated by further design development. For example, the top sequence contributing to LRF is an ATWS sequence where containment fails due to overpressure. Second to this is a Reactor Vessel Rupture (RVR) sequence where containment fails due to overpressure caused by the rupture-induced pressure surge which over-pressurises containment. This indicates the need to assess the ultimate containment fragility in order to replace the assumptions being used.

15.6.8.6 Applications of the PSA

The BWRX-300 PSA activities are ongoing as the design progresses to maturity. As demonstrated above, PSA insights have been a vital input to the design development. As the design and models evolve, the PSA will continue to be used to risk inform in the following ways:

- Demonstrate a balanced design that no particular feature or postulated IE makes a disproportionate contribution to overall risk
- Provide confidence of no cliff-edge effects
- Identify facility vulnerabilities and systems where design improvements or modifications to operational procedures could reduce probabilities of SAs or mitigate consequences
- Assess adequacy of emergency operating procedures
- Provide insights into SA management
- Inform test and maintenance arrangements

- Inform operating and emergency procedure development

Table 15.6- 1: Probabilistic Safety Assessment Objectives

#	Objectives of the PSA	Comments
1	To provide a systematic analysis giving confidence that the reactor facility's design aligns with the fundamental safety objectives as established in IAEA No.SF-1, Fundamental Safety Principles, including to protect people and the environment from radiation	Overarching objective
2	To demonstrate that a balanced design has been achieved; this can be demonstrated as achieved if no particular feature or postulated IE makes a disproportionately large or significantly uncertain contribution to the overall risk	Is demonstrated 008N9751 (Reference 15.6-10)
3	To provide confidence that small changes of conditions that may lead to a catastrophic increase in the severity of consequences (cliff-edge effects) are prevented	Is demonstrated in 008N9751 (Reference 15.6-10) and in the Sensitivity and Uncertainty Analysis
4	To provide assessments of the quantitative safety goals (the probabilities of occurrence for severe core damage states, and the assessments of the risks of radioactive releases to the environment) as defined in the ASME/ANS PSA standards for Level 1 (Reference 15.6-14) and Level 2 PSA (Reference 15.6-15), and IAEA-TECDOC-1804 (Reference 15.6-25), or as established in licensing basis for the facility	Is demonstrated in the results and discussion of Level 1 and 2 PSA.
5	To provide site-specific assessments of the probabilities of occurrence, and the consequences of external hazards	In the site-specific PSA
6	To identify facility vulnerabilities and systems for which design improvements or modifications to operational procedures could reduce the probabilities of SAs, or mitigate their consequences	Is demonstrated 008N9751 (Reference 15.6-10), and the sensitivity and uncertainty analysis
7	To assess the adequacy of emergency operating procedures	Licensee activity using the PSA results and insights
8	To use risk insights and results to inform SA management decisions	Licensee activity using the PSA results and insights

Table 15.6- 2: BWRX-300 Operational Modes

Mode	Description	Reactor Mode Switch Position	Notes	PSA Model
1	Power operation	Run	Fully pressurised and able to turn main turbine	FPIE
2	Startup	Refuel or startup	Reactor head fully tensioned, reactor trip system in startup configuration	Bounded by FPIE
3	Hot shutdown	Shutdown	Reactor head fully tensioned, scram signal received, and control rods inserted	LPSD
4	Stable shutdown	Shutdown	Reactor head fully tensioned, control rods inserted; mode can also be entered from cold shutdown to power operation	LPSD
5	Cold shutdown	Shutdown	Reactor head fully tensioned, control rods inserted; mode can also be entered from refuelling to power operation	LPSD
6-a	Refuelling (reactor cavity drained)	Shutdown or refuel	At least one reactor head stud NOT tensioned, containment assumed open	LPSD
6-b	Refuelling (reactor flooded to normal with the fuel pool gate installed)	Shutdown or refuel	At least one reactor head stud NOT tensioned, containment assumed open	LPSD
6-c	Refuelling (reactor flooded to normal with fuel pool gate removed)	Shutdown or refuel	At least one reactor head stud NOT tensioned, containment assumed open	LPSD

Table 15.6- 3: Safety Functions and Mitigating Systems – Full Power PSA

Fundamental Safety Function	Critical Safety Function	BWRX-300 Credited Systems
Reactivity control	Reactivity control	• Hydraulic SCRAM of control rods or • FMCRD SCRAM follow/motor run-in • FW runback control • Alternate boration with initial ICS operation, RPV pressure control, containment venting and injection.
Fuel cooling	Reactor pressure control (RPV pressure control is successful if RPV pressure is maintained at or below setpoint of ultimate pressure regulation.)	• Turbine bypass valves to main condenser (power conversion system) • Isolation Condenser System (ICS) • Ultimate Pressure Regulation (UPR) system
	Reactor coolant inventory control (Peak cladding temperature below 982°C)	• BOP via FW from the CST/condenser • CRD system
	Decay heat removal (Peak cladding temperature below 982°C)	• BOP via FW from the CST/condenser • ICS
Long term heat removal	Containment Integrity (including containment heat removal) (Containment failure assumed to occur at 3.5 times design pressure)	• ICS • Containment venting though Containment Overpressure Protection System (COPS) Note that, for containment heat removal, there are no sequences which can be mitigated by the PCCS in terms of its capacity
Containment integrity		• Containment isolation signals/valves/logic

Table 15.6- 4: Safety Functions Considered in the LPSD PSA

Fundamental Safety Function	Critical Safety Function	BWRX-300 Credited Systems
Reactivity control	Reactivity control	• Control rods are fully inserted and assumed to remain inserted int the shutdown model.
Fuel cooling	Reactor pressure control	• Isolation Condenser System (ICS) • Ultimate Pressure Regulation (UPR) system
	Reactor coolant inventory control	• CRD system (RPV injection • Equipment pool water transfer to reactor cavity (reactor cavity injection) • LWM system (reactor cavity injection) • FPS (spent fuel pool injection) • Flexible mitigation capability FLEX/EME (RPV injection)
	Decay heat removal	• ICS • SDC system
Long term heat removal	Containment Integrity (including containment heat removal)	• ICS • Containment venting though COPS
Containment integrity		• Containment Isolation signals/valves/logic

Notes:

- Reactor pressure control function is applicable to POS 3&4 and 5 as the reactor is open during POS 6-1 and 6-2.
- For reactor coolant inventory control, equipment pool water transfer is applicable to POS where RPV head is open and equipment pool and fuel pool gates are closed (i.e., POS 6-1). Reactor cavity injection from LWM is applicable to POS where RPV head is open (i.e., POS 6-1 and 6-2). Spent fuel pool injection via FPS is applicable to POS where RPV head is open and fuel pool gate is open (i.e., POS 6-2)).
- Containment integrity function is applicable to POS 3&4 as containment is open during POS 5, 6-1 and 6-2.
- The PCCS performs containment heat removal function. Since sequences that can be mitigated by the PCCS are very limited due to its capacity, the PCCS is not credited in the LPSD PSA.

Table 15.6- 5: Summary of Internal Hazards Screening to Determine Internal Hazards Taken Forward for Further Evaluation in the PSA

Hazard	Taken forward for assessment in PSA
Heavy load drop	• Yes – screened in qualitatively, forms part of fuel and heavy loads movements PSA and LPSD PSA.
Release of chemicals from on-site storage	• No – screened out qualitatively
Turbine-generated missiles	• No – screened out quantitatively
Other internally generated missiles	• No – Screened out qualitatively
Fires	• Yes – will be assessed as part of the internal fire PSA (not subject to screening)
Explosions	• Partially – components with explosion potential considered within scope of internal fire PSA. Explosions due to stored chemicals and combustibles screened out qualitatively.
Collapse of structures	• Partially – spontaneous collapse of structures housing mitigating equipment is screened out qualitatively. Collapse of structures in response to external events is included in the effects of the respective external hazard.
Pipe whips	• Yes – considered within the scope of the internal flooding PSA.
Jet effects	• Yes – considered within the scope of the internal flooding PSA.
Internal flooding	• Yes – will be assessed as part of the internal flooding PSA (not subject to screening)

Table 15.6- 6: FPIE CDF Uncertainty Result

Mean	5%	Median	95%
1.06E-08	9.44E-10	3.93E-09	3.38E-08

Table 15.6- 7: LP SD CDF Uncertainty Result

Mean	5%	Median	95%
1.31E-09	2.05E-10	6.07E-10	4.57E-09

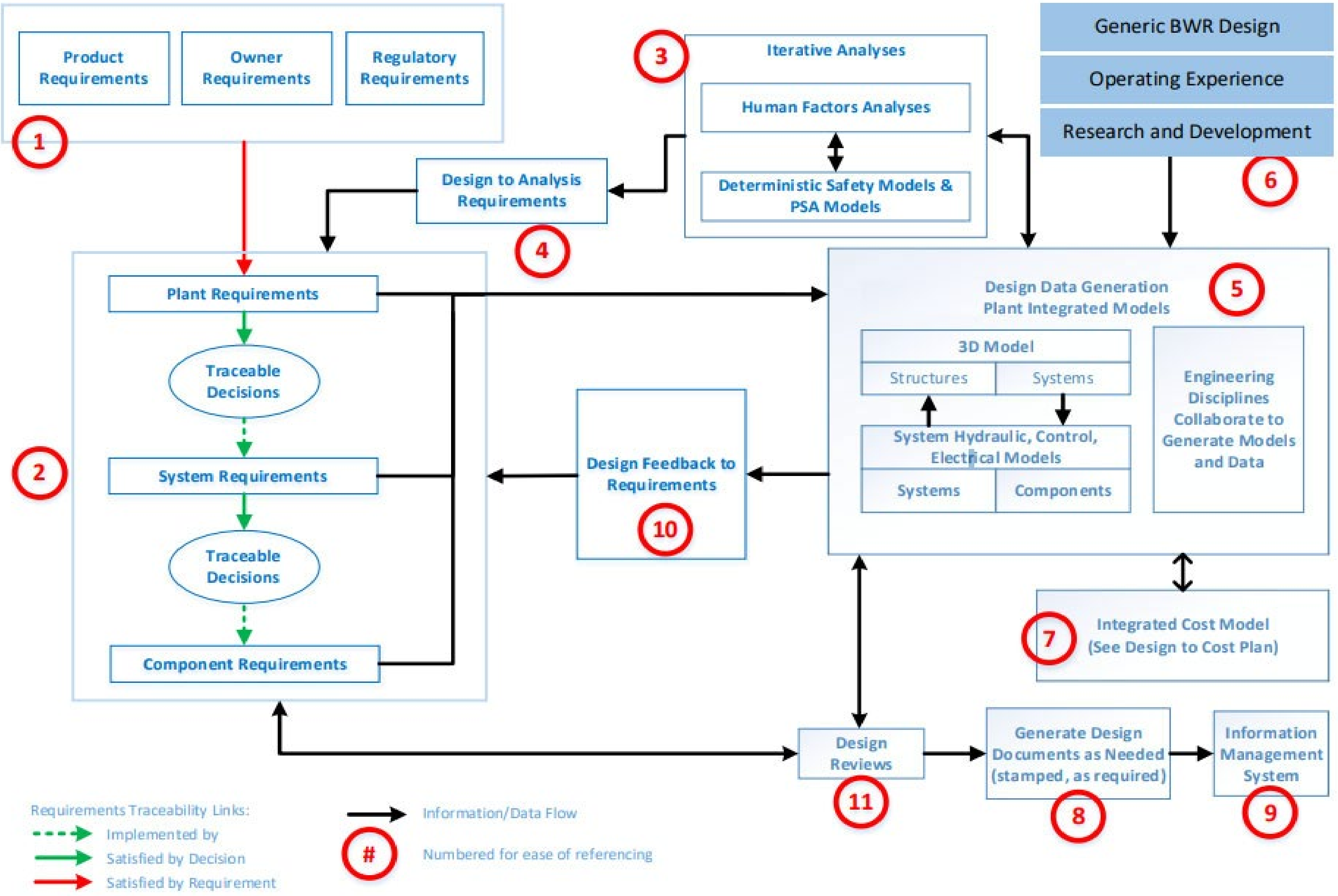

Figure 15.6- 1: Integrated Design Engineering Process

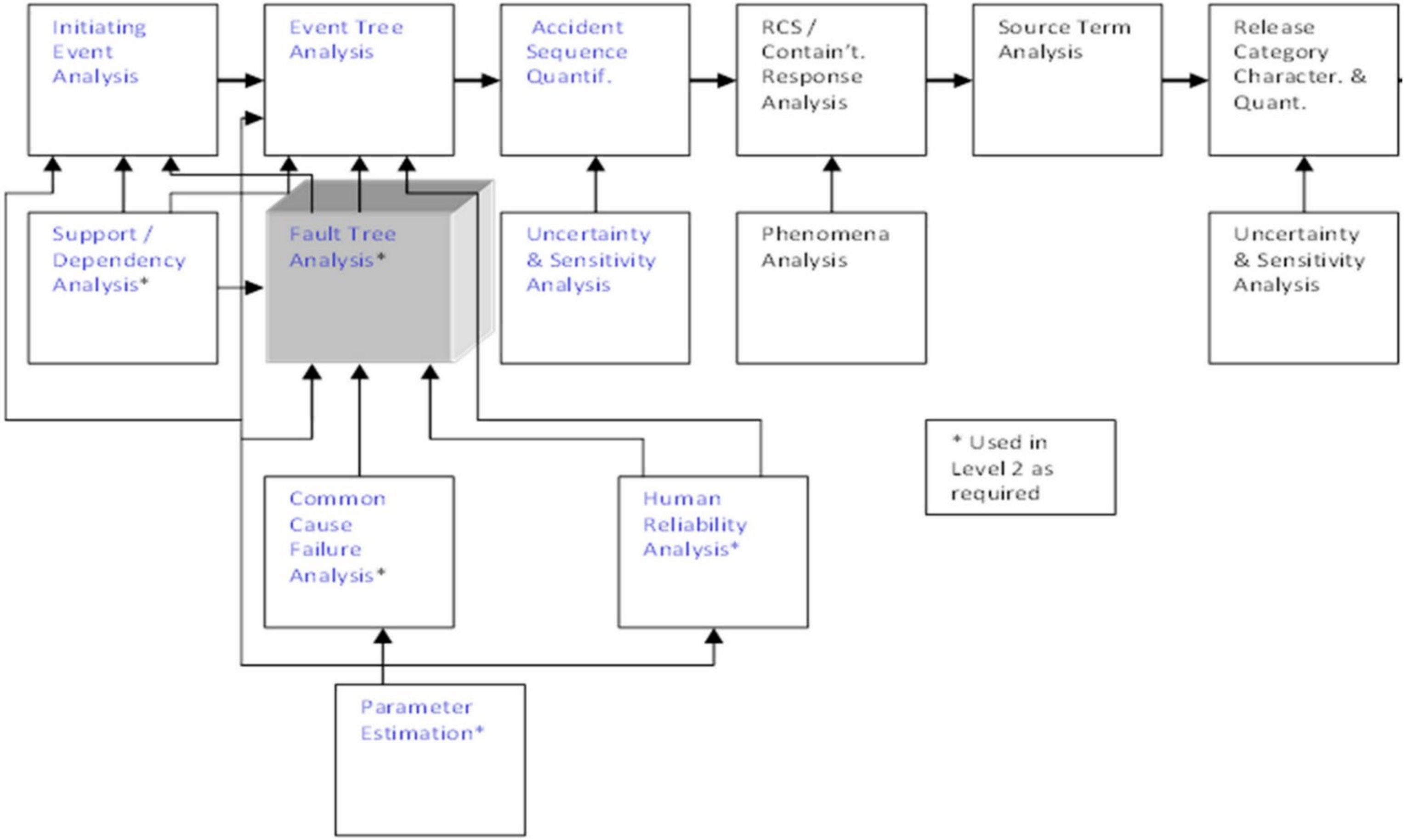
Initiating Event Analysis
Event Tree Analysis
Accident Sequence Quantif.
RCS / Contain't. Response Analysis
Source Term Analysis
Release Category Character. & Quant.
Support / Dependency Analysis*
Fault Tree Analysis*
Uncertainty & Sensitivity Analysis
Phenomena Analysis
Uncertainty & Sensitivity Analysis
* Used in Level 2 as required
Common Cause Failure Analysis*
Human Reliability Analysis*
Parameter Estimation*

Figure 15.6- 2: Principal Steps in Probabilistic Safety Assessment

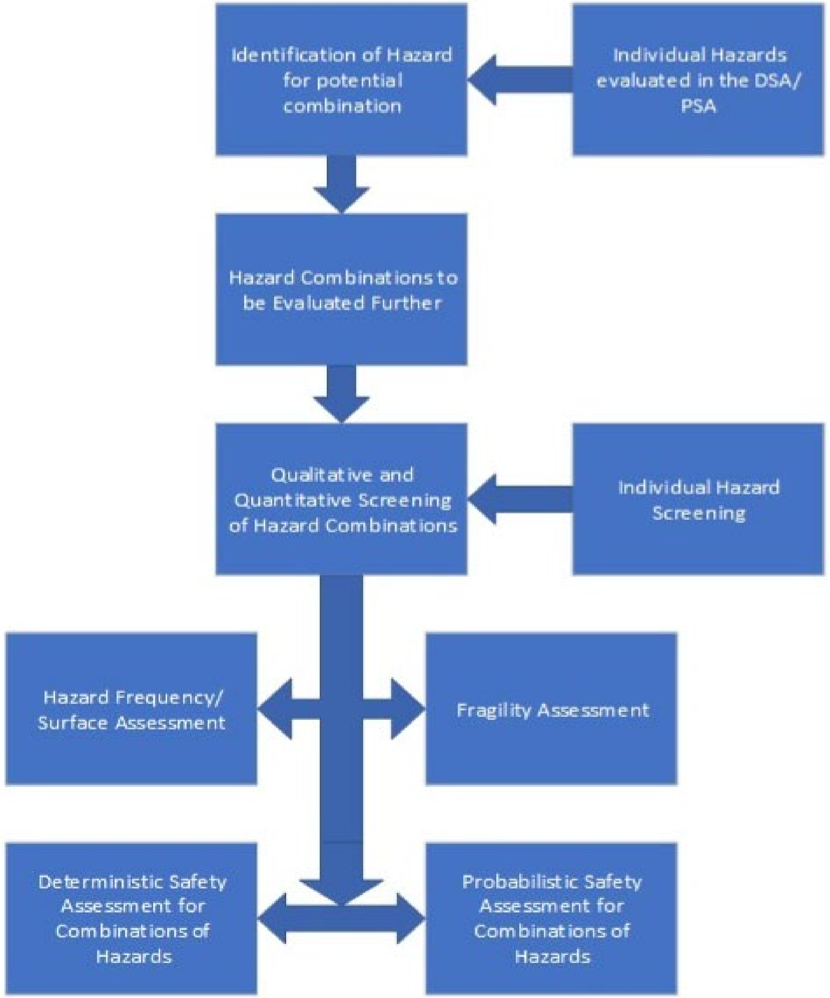
Identification of Hazard for potential combination
Individual Hazards evaluated in the DSA/ PSA
Hazard Combinations to be Evaluated Further
Qualitative and Quantitative Screening of Hazard Combinations
Individual Hazard Screening
Hazard Frequency/ Surface Assessment
Fragility Assessment
Deterministic Safety Assessment for Combinations of Hazards
Probabilistic Safety Assessment for Combinations of Hazards

Figure 15.6- 3: Overall Process for Selection, Screening and Analysis of Hazards

15.6.9 References

15.6-1 “Safety Assessment Principles for Nuclear Facilities”, Office for Nuclear Regulation, 2014 Edition, Revision 1 (January 2020).

15.6-2 NEDO-34179, “BWRX-300 UK GDA Subchapter 15.1: General Considerations of the BWRX-300 Safety Analysis,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-3 NEDO-34181, “BWRX-300 UK GDA Subchapter 15.3: Safety Objectives and Acceptance Criteria,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-4 NEDO-34182, “BWRX-300 UK GDA Subchapter 15.4: Human Actions,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC

15.6-5 NEDO-34185, “BWRX-300 UK GDA Subchapter 15.7: Internal Hazards,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC

15.6-6 NEDO-34186, “BWRX-300 UK GDA Subchapter 15.8: External Hazards,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-7 NEDO-34183, “BWRX-300 UK GDA Subchapter 15.5: Deterministic Safety Analysis,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-8 NEDO-34187, “BWRX-300 UK GDA Subchapter 15.9: Summary of Results,” Rev B, GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-9 006N2915, “BWRX-300 Standard Plant Probabilistic Safety Assessment Methodology,” GE-Hitachi Nuclear Energy, Rev 3, 2024.

15.6-10 008N9751, “UK BWRX-300 PSA Summary Report,” GE-Hitachi Nuclear Energy, Rev 1, 2024.

15.6-11 006N5064, “BWRX-300 Safety Strategy,” GE-Hitachi Nuclear Energy, Rev 6, 2024.

15.6-12 006N3139, “BWRX-300 Design Plan,” GE-Hitachi Nuclear Energy, Revision 5, 2023.

15.6-13 IAEA-TECDOC-1874, “Hierarchical Structure of Safety Goals for Nuclear Installations,” International Atomic Energy Agency, 2019.

15.6-14 ASME/ANS-RA-S-1.1-2022, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk,” American National Standards Institute, American Society of Mechanical Engineers, American Nuclear Society, 2022.

15.6-15 ASME/ANS-RA-S-1.2-2024, “Severe Accident Progression and Radiological Release (Level 2) PRA Standard for Nuclear Power Plant Applications for Light Water Reactors (LWRs),” American Society of Mechanical Engineers, 2024.

15.6-16 IAEA SSG-3, “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants,” International Atomic Energy Agency.

15.6-17 IAEA SSG-4, “Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants,” International Atomic Energy Agency.

15.6-18 EPRI 3002010659, “FRANX,” Electric Power Research Institute, Version 4.4, 2017.

15.6-19 EPRI 3002020050, “Phoenix Architect Module,” Electric Power Research Institute, Version 1.0b, 2020.

15.6-20 EPRI 3002010680, “The EPRI Human Reliability Analysis Calculator Software Manual,” Electric Power Research Institute, 2017.

15.6-21 EPRI 3002000578, “Uncertainty Evaluation Tool (UNCERT),” Electric Power Research Institute, Version 4.0, 2014.

15.6-22 FTREX Software, Electric Power Research Institute.

15.6-23 NEDO-11209-A, “Quality Assurance Program Description,” GE-Hitachi Nuclear Energy, 2022.

15.6-24 ASME 58.22-2014, “Requirements for Low Power and Shutdown Probabilistic Risk Assessment [Standard for Trial Use],” American Society of Mechanical Engineers, 2017.

15.6-25 IAEA-TECDOC-1804, “Attributes of Full Scope Level 1 Probabilistic Safety Analysis,” International Atomic Energy Agency, 2016.

15.6-26 EPRI ALWR URD NP-2230, “EPRI-ALWR Utility Requirements Document,” Electric Power Research Institute, Revision 4, 1992.

15.6-27 NUREG/CR-5750, “Rates of Initiating Events at U.S. Nuclear Power Plants:1987-1995,” U.S. Nuclear Regulatory Commission, Idaho National Laboratory, 1999.

15.6-28 NUREG/CR-6928, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,” 2015.

15.6-29 005N3558, “BWRX-300 Fault Evaluation,” GE-Hitachi Nuclear Energy, Revision 1.

15.6-30 EPRI TR-1016741, “Support System Initiating Events, Identification and Quantification Guideline,” Electric Power Research Institute, 2008.

15.6-31 NUREG/CR-2300, “PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, American Nuclear Society, Institute of Electrical and Electronics Engineers, 1983.

15.6-32 NUREG/CR-4550, “Analysis of Core Damage Frequency: Surry, Unit 1 Internal Events Appendices,” U.S. Nuclear Regulatory Commission, Sandia National Laboratory, 1990.

15.6-33 NUREG/CR-4551, “Evaluation of Severe Accident Risks: Methodology for the Containment, Source Term, Consequence, and Risk Integration Analyses,” U.S. Nuclear Regulatory Commission, Sandia National Laboratory, 1993.

15.6-34 NUREG-0492, “Fault Tree Handbook,” U.S. Nuclear Regulatory Commission, 1981.

15.6-35 “Overview of the PRA Process and Basic PRA Techniques,” Idaho National Laboratory, https://www.nrc.gov/docs/ML1216/ML12160A310 , 2012.

15.6-36 EPRI TR-016780-V3R8, “Advanced Light Water Reactor Utility Requirements Document, Volume 3,” Electric Power Research Institute, Revision 8: ALWR Passive Plant.

15.6-37 “CCF Parameter Estimations, 2020 Update,” U.S. Nuclear Regulatory Commission, Revision 1, https://nrcoe.inl.gov/publicdocs/CCF/CCFParameterEstimates2020Rev1.xlsx .

15.6-38 “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, https://nrcoe.inl.gov/publicdocs/AvgPerf/ParameterEstimates2020.xlsx , 2020.

15.6-39 NEDE-22056, “Failure Rate Data Manual for GE BWR Components,” GE-Hitachi Nuclear Energy, Revision 2.

15.6-40 INEEL/EXT-98-00892, “Selected Component Failure Rate Values from Fusion Safety Assessment Tasks,” 1998.

15.6-41 NUREG/CR-5500, “Reliability Study: General Electric Reactor Protection System 1984-1995,” U.S. Nuclear Regulatory Commission, Idaho National Engineering and Environmental Laboratory, Vol. 3, 1999.

15.6-42 NUREG/IA-0463, “(Availability of) An International Report on Safety Critical Software for Nuclear Reactors by the Regulator Task Force on Safety Critical Software (TF-SCS),” U.S. Nuclear Regulatory Commission, 2015.

15.6-43 NUREG/CR-6268, INL/EXT-07-12969, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding,” U.S. Nuclear Regulatory Commission, Idaho National Laboratory, 2007.

15.6-44 NEDC-34158P, “BWRX-300 UK GDA Probabilistic Safety Assessment Strategy,” GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-45 NUREG-1738, “Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Plants,” U.S. Nuclear Regulatory Commission, 2001.

15.6-46 IAEA SSG-64, “Protection against Internal Hazards in the Design of Nuclear Power,” International Atomic Energy Agency, 2021.

15.6-47 IAEA SSG-3, “Development and Application of Level 1 Probabilistic Safety Assessment,” International Atomic Energy Agency, 2010.

15.6-48 ASME/ANS RA-S-1.4 – 2021, “Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants,” ASME/ANS Joint Committee on Nuclear Risk Management, 2021.

15.6-49 EPRI 1011989 NUREG/CR-6850, “Fire PRA Methodology for Nuclear Power Facilities,” Electric Power Research Institute, U.S. Nuclear Regulatory Commission, 2005.

15.6-50 NUREG/CR-6850 Supplement 1, EPRI 1019259, “Fire Probabilistic Risk Assessment Methods Enhancements,” Electric Power Research Institute, U.S Nuclear Regulatory Commission, 2010.

15.6-51 NUREG-2169, EPRI 3002002936, “Nuclear Power Plant Fire Ignition Frequency and Non-Suppression Probability Estimation Using the Updated Fire Events Database,” Electric Power Research Institute, U.S. Nuclear Regulatory Commission, 2015.

15.6-52 NUREG-2230, EPRI 3002016051, “Methodology for Modelling Fire Growth and Suppression Response for Electrical Cabinet Fires in Nuclear Power Plants,” Electric Power Research Institute, U.S. Nuclear Regulatory Commission, 2020.

15.6-53 NUREG/CR-4639, “Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR),” U.S. Nuclear Regulatory Commission, Rev 1, 1990.

15.6-54 NUREG/CR-6890 Vol 1, INL/EXT-05-00501 Vol 1, “Re-evaluation of Station Blackout Risk at Nuclear Power Plants, Vol. 1, Analysis of Loss of Offsite Power Events: 1986-2004,” U.S. Nuclear Regulatory Commission, 2005.

15.6-55 “Enhanced Fujita Scale (EF-Scale)”, Wind Science and Engineering Center, 10 October 2006. [Online]. Available: http://www.spc.noaa.gov/faq/tornado/EFScale.pdf [Accessed 3 August 2017].

15.6-56 NUREG/CR-4461 Rev 2, PNNL-15112, “Tornado Climatology of the Contiguous United States,” U.S. Regulatory Commission, Rev 1, 2007.

15.6-57 EPRI 3002008092, “High Wind Equipment List and Walkdown Guidance,” Electric Power Research Institute, 2016.

15.6-58 NUREG/CR-7004, “Technical Basis for Regulatory Guidance on Design-Basis Hurricane-Borne Missile Speeds for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, 2011.

15.6-59 NUREG/CR-7005, “Technical Basis for Regulatory Guidance on Design-Basis Hurricane Wind Speeds for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, 2011.

15.6-60 “Modular Accident Analysis Program for LWR Power Plants, Transmittal Document for MAAP5 Code,” Electric Power Research Institute, Revision MAAP 5.05, 2019.

15.6-61 EPRI TR-1009652, “Guideline for the Treatment of Uncertainty in Risk Informed Applications: Technical Basis Document,” Electric Power Research Institute, 2004.

15.6-62 EPRI TR-1013491, “Guideline for the Treatment of Uncertainty in Risk Informed Applications: Applications Guide,” Electric Power Research Institute, 2006.

15.6-63 EPRI TR-1016737, “Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments,” Electric Power Research Institute, 2008.

15.6-64 NUREG-1855, “Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making,” U.S. Nuclear Regulatory Commission, Revision 1, 2017.

15.6-65 EPRI TR-1026511, “Practical Guidance on the Use of Probabilistic Risk Assessment in Risk-Informed Applications with a Focus on the Treatment of Uncertainty,” Electric Power Research Institute, 2012.

15.6-66 NEDC-34357P, “BWRX-300 UK GDA Safety Case Manual Specification”, GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-67 NEDC-34140P, “BWRX-300 UK GDA Safety Case Development Strategy,” GE-Hitachi Nuclear Energy, Americas, LLC.

15.6-68 NEDC-34138P, “BWRX-300 UK GDA Generic Site Envelope and External Hazards Identification,” GE-Hitachi Nuclear Energy, Americas, LLC.

APPENDIX A CLAIMS, ARGUMENTS AND EVIDENCE

A.1 Claims, Arguments and Evidence

The ONR SAPs 2014 (Reference 15.6-1) identify ONR's expectation that a safety case should clearly set out the trail from safety claims, through arguments to evidence. The Claims, Arguments, Evidence (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 Claims, Arguments, Evidence structure is defined within the NEDC-34140P "BWRX-300 UK GDA Safety Case Development Strategy," (Reference 15.6-67) and is a logical breakdown of an 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 1 claim is:

> 2 *"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 subchapter will mainly support the Level 2 claim, which is:

> 1.3 *"A suitable and sufficient safety analysis has been undertaken which presents a comprehensive faut and hazard analysis that specifies the requirements on the safety measures and informs emergency arrangements. (Safety Analysis)"*

The Level 3 sub-claim relevant to this Level 2 claim is as follows:

> 1.3.4 *Probabilistic Safety Assessment is carried out to reflect the BWRX design and evaluate the risk levels.*

This subchapter will also directly support a secondary Level 2 claim, which is:

> 1.3 *"Safety risks have been reduced as low as reasonably practicable."*

The Level 3 sub-claim relevant to this Level 2 claim is as follows:

> 2.4.1 *Relevant Good Practice (RGP) has been taken into account across all disciplines.*
>
> 2.4.2 *Operational Experience (OPEX) and Learning from Experience (LfE) has been taken into account across all disciplines.*
>
> 2.4.3 *Optioneering (all reasonably practicable measures have been implemented to reduce risk)*

2.4.4 Residual risks are compared with numerical targets and no event sequences are disproportionately dominant.

In order to facilitate compliance, demonstration against the above Level 3 sub-claim, this PSR subchapter has derived a suite of arguments that comprehensively explain how their applicable Level 3 sub-claim is met (see Table A-1 below).

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 2-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, this subchapter contributes to the overall future ALARP case by demonstrating that that the subchapter-specific arguments derived may be supported by existing and future planned evidence for the arguments in Table A-1.

Table A-1: PSA Claims and Arguments

Subchapter 15.6 Claim	Subchapter 15.6 Argument	Sub-sections and/or reports that evidence the arguments:
2.3 A suitable and sufficient safety analysis has been undertaken which presents a comprehensive faut and hazard analysis that specifies the requirements on the safety measures and informs emergency arrangements. (Safety Analysis)”		
2.3.4 Probabilistic Safety Assessment is carried out to reflect the BWRX design and evaluate the risk levels	A full scope PSA model is under development, with an iterative approach undertaken to ensure that the model is updated in line with design development.	15.6 General Approach to Probabilistic Safety Assessment NEDC-34158P (Reference 15.6-44) UK BWRX-300 PSA Methodology (Reference 15.6-9) 008N9751 (Reference 15.6-10)
	The results and associated risk insights produced by the PSA models have been interrogated and used to inform the BWRX design and development process. Future iterations will be used to inform emergency arrangements.	15.6.6 Results of The Level 1 Probabilistic Safety Assessment 15.6.7 Results of The Level 2 Probabilistic Safety Assessment 15.6.8 Probabilistic Safety Assessment Insights and Applications 008N9751 (Reference 15.6-10)
2.4 Safety risks have been reduced as low as reasonably practicable		
2.4.1 RGP has been taken into account across all disciplines	The PSA is developed in accordance with the ASME/ANS standards. Other international guidance, such as IAEA guidance, is taken into account throughout the PSA development.	15.6 General Approach to Probabilistic Safety Assessment
2.4.2 OPEX and Learning from Experience has been taken into account across all disciplines	OPEX and learning from experience feeds into the fault identification process and data analysis that is undertaken for the PSA. Generic data sources are produced by the collection of data from across the industry. Guidance documents that have been used to	15.6 General Approach to Probabilistic Safety Assessment 15.6.1.2 Initiating Events Analysis 15.6.1.5 Data Analysis

Subchapter 15.6 Claim	Subchapter 15.6 Argument	Sub-sections and/or reports that evidence the arguments:
	support the BWRX PSA development have been produced by subject experts and have been enhanced over time, taking OPEX and learning into account. It is noted that many of the traditionally high-risk faults have been designed out or minimized in the BWRX design and this is reflected in the low CDF that has been calculated.	15.6.2.1 Internal Hazards
2.4.3 Optioneering (all reasonably practicable measures have been implemented to reduce risk)	Development of the PSA has led to a number of risk insights which have been fed back into the design as part of the BWRX integrated design engineering process. Optioneering is conducted as part of the design review process and all key stakeholders, including the PSA team, are involved to ensure that the risk is as low as reasonably practicable.	15.6.8 Probabilistic Safety Assessment Insights and Applications NEDC-34158P (Reference 15.6-44)
2.4.4 Residual risks are compared with numerical targets and no event sequences are disproportionately dominant	Numerical risk and dose targets have not been established at this stage of the GDA process. Development of such targets and the Level 3 PSA is on the FAP. However, the PSA demonstrates low risk when compared to the plant safety goals for CDF and LRF, especially considering the level of conservatisms at this stage in development. Furthermore, any significant contributing sequences to risk are analysed and risk insights are fed back into the design to inform further design improvements.	15.6.6 Results of The Level 1 Probabilistic Safety Assessment 15.6.7 Results of The Level 2 Probabilistic Safety Assessment 15.6.8 Probabilistic Safety Assessment Insights and Applications 008N9751 (Reference 15.6-10)

APPENDIX B FORWARD ACTIONS

Table B-1: PSA Forward Actions

Action ID	Finding	Forward Actions	Delivery Phase
PSR15.6 - 39	The safety goals that are currently set for the BWRX look at core damage frequency and large release frequency. Whilst these are useful metrics to assess, they do not allow comparison with the UK Safety Assessment Principles (SAP) Numerical Targets 7- 9, which is essential to meet UK expectations. Worker risk (on-site) targets, equivalent to SAP Targets 5 and 6, are also required.	The safety goals that are currently set for the BWRX look at Core Damage Frequency and Large Release Frequency. Whilst these are useful metrics to assess, they do not facilitate a comparison to be made with the UK SAP Numerical Targets. To facilitate this comparison and provide a means to show alignment with the relevant SAP Numerical Targets, dose and risk based targets will be developed for the UK BWRX against which to assess the results of the Level 3 PSA.	For Pre-Construction Safety Report (PCSR)/Pre-Construction Environment Report (PCER)
PSR15.6 - 40	There is currently no PSA Level 3 analysis that meets UK expectations.	A best estimate Level 3 PSA will be developed to assess the on and offsite consequences of all potential radiological releases from the site in order to allow assessment against numerical targets equivalent to SAP Targets 5 – 9. This will be a full scope assessment including all operating modes and both internal and external hazards. Initial assessment will be made using data for a bounding site. Once a site is selected, site specific data (meteorological, population, agricultural) can be used to produce a full Level 3 PSA assessment.	For PCSR/PCER
PSR15.6 - 41	Currently sequences that could potentially result in a small off-site release but that are not taken forward to the Level 2 PSA are not identified and quantified.	In order to support the Level 3 PSA development, source terms and frequencies will be calculated for all potential releases,	For PCSR/PCER

Action ID	Finding	Forward Actions	Delivery Phase
		including all that could result in an effective dose of 0.1 mSv or above for a hypothetical person at most risk off-site (or 2 mSv on-site). This will include non-core damage sequences which were not taken forward to the Level 2 PSA and also potentially non-reactor faults which were screened out of the Level 1 PSA (e.g., waste facilities).	
PSR15.6 - 42	Currently the Level 2 PSA is not fully developed for all modes, events, and hazards. In addition, it has been set up for the large release category metric only and therefore may not have the required characteristics necessary to meet the Level 3 PSA UK requirements.	Further development of the Level 2 PSA, with supporting severe accident analysis and containment performance analysis to be undertaken for all operating modes and all initiating events. Full development of the external hazard PSA to be completed on site selection.	For PCSR/PCER
PSR15.6 - 43	The current hazard prioritisation has not been performed taking into consideration UK site characteristics.	Using the generic site envelop development and external hazard identification presented in NEDC-34148P, “BWRX-300 UK GDA Generic Site Envelope and External Hazards identification,” (Reference 15.6-68) as a starting point, perform the external hazard prioritisation for the UK context. This can be further developed on site selection.	For PCSR/PCER
PSR15.6 - 44	Site specific external hazards PSA needs to be performed, including hazard characterisation through site specific hazard curve development.	On completion of the external hazard prioritisation/screening task and identification of external hazards to be taken forward for further analysis in the PSA, site specific PSA will be developed for these hazards. This will include development of appropriate hazard curves representing the chosen UK site	For Site License Application

Action ID	Finding	Forward Actions	Delivery Phase
		characteristics. This will involve, but is not limited to, seismic and high wind hazards.	
PSR15.6 - 45	External-external and external-internal hazard combinations need to be evaluated in the PSA, following the hazard prioritisation assessment.	All credible hazard combinations that might affect the UK site should be identified. Consideration should be given to consequential, correlated, and independent hazard combination types. Once appropriate screening or bounding assessment has been performed, determine those hazard combinations requiring further detailed assessment in the PSA.	For PCSR/PCER
PSR15.6 - 46	HRA for operator actions significant to internal flood needs to be performed. This can then support the analysis of recovery/mitigation of flooding events by operator actions. Whilst conservative, at this stage flood source isolation has not been considered in the modelling. High energy line break consequences such as pipe-whip/jets/impactive force from flooding source have not been modelled. Once the analysis moves away from all target damage in flood source PAU, this will become more significant.	The internal flooding PSA will be further developed as the plant design matures and details on procedures become available. More specifically, HRA for operator actions identified as being significant to internal flood needs to be performed. This can then support the analysis of recovery / mitigation of flooding events by operator actions. Whilst conservative, at this stage flood source isolation has not been considered in the modelling. High energy line break consequences such as pipe-whip / jets / impactive force from flooding source will be considered. Once the analysis moves away from all target damage in flood source PAU, this will become more significant.	For PCSR/PCER
PSR15.6 - 47	The fire PSA follows the guidance set out in NUREG/CR-6850 (Reference 15.6-49). Being a design stage PSA and due to a lack of detailed information, some of the fire tasks could not be performed:	The internal fire PSA will be further developed as the plant design matures and the necessary detailed information becomes available. The internal fire PSA follows the guidance set	For PCSR/PCER

Action ID	Finding	Forward Actions	Delivery Phase
	ask 9 Detailed circuit failure analysis ask 10 Detailed Circuit Failure Mode and Likelihood Analysis ask 11 Detailed Fire Modelling - A) Single Compartment, B) Multi-Compartment, C) MCR	out in NUREG/CR-6850 and the following fire PSA tasks will be developed and performed: -Task 9 Detailed circuit failure analysis -Task 10 Detailed Circuit Failure Mode and Likelihood Analysis -Task 11 Detailed Fire Modelling - A) Single Compartment, B) Multi-Compartment, C) MCR	
PSR15.6 - 48	Preliminary sensitivity calculations have been undertaken to look at the impact of considering the passive reliability of the ICS, using values from the example study presented in IAEA-TECDOC-1752. However, consideration of the passive reliability has not been included in the base model.	It is generally accepted across the industry that passive system reliability is a developing area of nuclear safety engineering and at the moment there is no established benchmark for relevant good practice in this area. Notwithstanding, a passive reliability assessment of the BWRX-300 ICS will be conducted to ensure that a best estimate can be included in the PSA. This will be based on the approach presented in IAEA-TECDOC-1752 or another relevant, industry accepted source and will consider the plant specific thermal hydraulic analysis.	For PCSR/PCER
PSR15.6 - 49	Although the event tree structure has been developed in a symmetrical way, certain assumptions in the fault trees (e.g., relating to running/standby pumps), make this a non-symmetrical model. In order to be ready to be used for certain applications such as risk monitors, the model must be fully symmetrical.	Ensure model is fully symmetrical as appropriate for use with a risk monitor by fully developing assumptions relating to running/standby pumps.	For Site License application
PSR15.6 - 50	The frequency, duration and nature of test and maintenance activities have not yet been fully determined. Therefore, generic data and informed judgements have been made where necessary to include unavailability due to test and maintenance activities.	A systematic review will be conducted for all systems as more information becomes available regarding test and maintenance activities so that these can be fully accounted	For Site License application

Action ID	Finding	Forward Actions	Delivery Phase
		for in the model when modelling unavailability due to test and maintenance.	
PSR15.6 - 51	Test intervals are not currently accounted for in the component reliability models.	Once the testing procedures have been developed, the test intervals will be incorporated into the component reliability models as appropriate.	For Site License application
PSR15.6 - 52	LOCA frequencies by size (i.e., small, medium, large) are based on the generic data source's definition. However, BWRX-300 needs to develop size delineation based on a design-specific analysis.	LOCA frequencies are currently based on generic data sources. Once stable BWRX-300 piping design information is available, including piping length, piping size, and valve locations in containment, the plant specific LOCA frequencies can be calculated. The excessive LOCA frequency (reactor vessel rupture) may also be refined. In addition, the functional break categories based on BWRX success criteria may differ from the data source in terms of small, medium and large designation and this discrepancy will be addressed when using the plant specific information.	For PCSR/PCER
PSR15.6 - 53	A spurious UPR pathway opening initiating event is not included in the GDA step 2 model.	Spurious UPR pathway opening leading to LOCA will be analysed in the PSA.	For PCSR/PCER
PSR15.6 - 54	The current initiating event analysis was based on FMEAs and design information available at the time. However, as the design continues to evolve systematic review is required to ensure that all potential initiating events have been identified.	Additional FMEAs and detailed reviews for potential system initiators will be conducted, as the design evolves.	For PCSR/PCER
PSR15.6 - 55	The failure of alarms and indications for operator actions is not currently modelled.	When developing Type C operator actions as more information becomes available, alarms and indications will be explicitly modelled, if	For PCSR/PCER

Action ID	Finding	Forward Actions	Delivery Phase
		judged necessary, to ensure that all dependencies are correctly captured.	
PSR15.6 - 56	The assumed designs of the UPR system and COPS have direct impact on the success of containment. The assumed ultimate pressure capability of the BWRX-300 is based on historical analysis of other BWR containments. Other design assumptions have been made as input into the initial success criteria analysis.	All assumptions used in the success criteria analysis will be reviewed as the design is developed and will also be used to inform design development. - The PSA team continue to be involved in the design optioneering of the UPR and COPS systems and the model and analysis will be updated as the design evolves. - The containment pressures in the excessive LOCA and Large LOCA will be considered in the design of the COPS. - The pressure capability assumption is most important for the RVR sequences and will be reviewed when design and analysis of the BWRX-300 containment is completed. - The CRD flow capacity and the flowrate in response to maintaining RPV inventory/level will be reviewed as the design develops.	For Site License application
PSR15.6 - 57	Modelling of ATWS scenarios The current ATWS modelling includes many conservative assumptions relating to the success criteria.	Thermal hydraulic analysis of ATWS sequences using TRACG has been undertaken and will continue to be developed. This analysis will be used to further refine the ATWS sequences and success criteria assumptions in the PSA model. Development of the success criteria will consider the potential to credit the UPRs during ATWS events, which would reduce the current conservatisms.	For PCSR/PCER

Action ID	Finding	Forward Actions	Delivery Phase
PSR15.6 - 58	The HVS system is currently not modelled in the PSA model. In order to accurately understand the success criteria for the HVS system, room heat up calculations are required.	Once the HVS design is sufficiently understood, room heat-up calculations will be performed to support success criteria development for HVS and to support external hazard analysis. The fault tree modelling for the HVS systems will be developed.	For PCSR/PCER
PSR15.6 - 59	The GDA model is based on an old I&C design which included an analogue hardware platform for DL4a I&C	The I&C system analysis will be updated to align with the new system design. The level of detail in the fault tree modelling will be increased as the design advances, using a newly developed methodology for I&C modelling.	For PCSR/PCER
PSR15.6 - 60	No peer review has yet been undertaken of the PSA model.	Peer review to be undertaken once the full scope PSA has been developed. This will assess against UK ONR TAGs and ASME/ANS standards.	For Site License application
PSR15.6 - 61	The PSA methodology is captured in the methodology report. Task procedures have not yet been developed for each individual task.	Detailed task procedures will be developed for each PSA task to ensure consistency in approach going forward as the model continues to be developed.	For PCSR/PCER