Office for Nuclear Regulation

ONR Assessment Report

Generic Design Assessment of the BWRX-300 – Step 2 Assessment - Fault Studies and Severe Accident Analysis

ONR Assessment Report

Project Name: Generic Design Assessment of the BWRX-300 – Step 2

Report Title: Step 2 Assessment of Fault Studies and Severe Accident Analysis

Authored by: Nuclear Safety Inspector, ONR

Assessment report reference: AR-01348

Project report reference: PR-01880

Report issue: 1

Published: December 2025

Document ID: ONRW-2126615823-7711

Executive summary

In December 2024, the Office for Nuclear Regulation (ONR), together with the Environment Agency and Natural Resources Wales, began Step 2 of the Generic Design Assessment (GDA) of the BWRX-300 design on behalf of GE Vernova Hitachi Nuclear Energy International LLC, United Kingdom (UK) Branch, the Requesting Party (RP).

This report presents the outcomes of my Fault Studies & Severe Accident Analysis assessment of the BWRX-300 design as part of Step 2 of the ONR GDA. This assessment is based upon the information presented in the RP's safety, security, safeguards and environment cases (SSSE), the associated revision 3 of the Design Reference Report and supporting documentation.

ONR's GDA process calls for an assessment of the RP's submissions, which increases in detail as the project progresses. The focus of my assessment in this step was to support ONR's decision on the fundamental adequacy of the BWRX-300 design and safety case, and the suitability of the methodologies, approaches, codes, standards and philosophies which form the building blocks for the design and generic safety, security and safeguards cases.

I targeted my assessment, in accordance with my assessment plan, at the areas that were fundamental to the acceptability of the design and methods for deployment in GB (Great Britain), benchmarking my regulatory judgements against the expectations of ONR's Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAGs) and other guidance which ONR regards as relevant good practice, such as IAEA (International Atomic Energy Agency) safety standards. Where appropriate, I have also considered how I could use relevant learning and regulatory conclusions from the UK ABWR GDA to inform my assessment of the BWRX-300.

I targeted the following aspects in my assessment of the BWRX-300 SSSE:

- Adequacy of approach and implementation of Defence in Depth, Safety Categorisation and Classification;
- Fault analysis approach to design basis and beyond design basis events;
- Identification of faults and event sequences;
- Effectiveness of design basis safety measures;
- Approach to severe accident analysis and feasibility of severe accident safety features;
- The RP's approach to fault analysis of non-reactor faults, start-up and shutdown faults;

- Radiological consequence assessment;
- Validation of computer codes;
- Practical elimination of sequences with the potential to lead to large or early release; and
- Enabling risks reduced ALARP (As Low As Reasonably Practicable).

My assessment scope has largely been limited to power operations of the BWRX-300. Based upon my assessment, I have concluded the following:

- The RP's approach to defence in depth and safety categorisation and classification is adequate;
- The RP's approach to fault analysis provides a robust demonstration of multiple layers of defence in depth;
- The RP's methodology for initiating event and sequence identification is adequate. However, I have identified some initiating events and sequences that require further justification for exclusion, a demonstration of protection against them, or design modifications to provide adequate protection. These concern large Loss of Coolant Accidents and the Reactor Isolation Valves as well as high reliability claims placed on shutdown systems using control rods and on the Isolation Condenser System. For all these sequences, I am content there are appropriate Forward Action Plans and have confidence the RP could make an adequate case in future;
- For design basis accident and design extension conditions with limited fuel damage sequences that the RP has identified, the deterministic analysis adequately demonstrates that the safety measures are sufficient to meet the RP's safety criteria;
- The RP's approach to severe accident analysis is appropriate in determining sufficient severe accident safety features, and the safety features feasibly prevent or mitigate appropriate phenomena;
- The RP has yet to apply its fault analysis approach to non-reactor faults, start-up and shutdown faults. However, the RP have presented some preliminary analysis which provides me with confidence in the methodologies that will be applied. I am content that there is a Forward Action Plan covering these faults and I have confidence that a future safety case could be made;
- No radiological consequence assessment has been undertaken, to date. However, since decoupled criteria are met for design basis faults, and based on the design of the BWRX-300, I am content this is covered by a Forward Action Plan and am confident that a future consequence

assessment would not hinder an adequate safety case from being made in future;

- The computer codes used to underpin design basis and severe accident analysis are adequately validated for use;
- An overall demonstration of practical elimination has not been provided, to date. However, the RP's approach to defence in depth and the deterministic analysis of safety measures provided for design basis and severe accident analysis provide confidence that an adequate case can be made in the future; and
- The RP's adoption of good practice to fault analysis and design development provides confidence that a demonstration of ALARP will be achievable in a future safety case subject to completing further work identified in its Forward Action Plans.

During my assessment, I have raised one Regulatory Observation regarding sequences that I judge should be considered in a future safety case. I am content that the Resolution Plan which the RP have produced demonstrates its understanding of the gap and has identified a credible means to resolve it.

Overall, based on my assessment to date, I have not identified any fundamental safety shortfalls that could prevent ONR permissioning the construction of a power station based on the generic BWRX-300 design; noting that any decision to permission a BWRX-300 will require further assessment (in either a future Step 3 GDA or during site specific activities) of suitable and sufficient supporting evidence that can substantiate the claims and proposals made in the GDA Step 2 submissions.

List of abbreviations

ALARP	As Low As Reasonably Practicable
ABWR	Advanced Boiling Water Reactor
AOO	Anticipated Operational Occurrences
APS	Anticipatory Protection System
BDBA	Beyond the Design Basis Analysis (a UK term which relates to SAA)
BTC	Basic Technical Characteristics
BWR	Boiling Water Reactor
CAE	Claims, Arguments and Evidence
CCF	Common Cause Failure
CDF	Core Damage Frequency
CN-DSA	Conservatively biased DSA
CNSC	Canadian Nuclear Safety Commission
CSAU	Code, Scaling, Applicability and Uncertainty
CVTR	Carolina Virginia Test Reactor
DBA	Design Basis Accident
DBA	Design Basis Analysis (a UK term which relates to DSA)
DAC	Design Acceptance Confirmation
DEC	Design Extension Conditions
DEC-A	DEC without core damage
DEC-B	DEC with core damage
DESNZ	Department of Energy Security and Net Zero
DiD	Defence in Depth
DNNP	Darlington New Nuclear Project
DR	Design Reference
DRP	Design Reference Point
DRR	Design Reference Report
DSA	Deterministic Safety Analysis
ESBWR	Economic Simplified Boiling Water Reactor
EX-DSA	DSA applied to the analysis of DEC
FAP	Forward Action Plan
FHA	Fuel Handling Accident (a US term)
FMCRD	Fine Motion Control Rod Drives
GB	Great Britain
GDA	Generic Design Assessment
GVHA	GE Vernova Nuclear Energy Americas LLC
GOTHIC	Generation of Thermal Hydraulic Information for Containments
GSE	Generic Site Envelope
GSR	Generic Security Report
IAEA	International Atomic Energy Agency
IC	Isolation Condenser
ICS	Isolation Condenser System
LfE	Learning from Experience
LOCA	Loss of Coolant Accident
LOPP	Loss of Preferred Power
LTR	Licensing Topical Report

LWR	Light Water Reactors
MAAP	Modular Accident Analysis Program
MCR	Main Control Room
MDSL	Master Document Submission List
MELCOR	A computer code developed for the NRC to model severe accidents
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NRW	Natural Resources Wales
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
OPG	Ontario Power Generation
PANTHERS	A full scale IC prototype used for qualification tests
PCCS	Primary Containment Cooling System
PCSR	Pre-construction Safety Report
PID	Project Initiation Document
PIE	Postulated Initiating Event
PIRT	Phenomena Identification and Ranking Table
PER	Preliminary Environmental Report
pfd	Probability of failure on demand
PSA	Probabilistic Safety Assessment
PSAR	Preliminary Safety Analysis Report
PSR	Preliminary Safety Report
RGP	Relevant Good Practice
RCPB	Reactor Coolant Pressure Boundary
RI	Regulatory Issue
RITE	Risk Informed Targeted Engagement
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
SAA	Severe Accident Analysis
SAFDLs	Specified Acceptable Fuel Design Limits
SAPs	Safety Assessment Principles
SCR	Secondary Control Room
SSSE	Safety, Security, Safeguards and Environment Cases
SMR	Small Modular Reactor
SSCs	Structures, Systems and Components
SFAIRP	So far as is reasonably practicable
SSC	Structure, System and Component
STP	Simulated Thermal Power
TAG	Technical Assessment Guide(s) (ONR)
TRACE	Transient Reactor Analysis Computational Engine
TRACG	Transient Reactor Analysis Code General Electric
TSC	Technical Support Contractor
TSV	Turbine Stop Valves
UK	United Kingdom
US	United States of America
WENRA	Western European Nuclear Regulators' Association

Contents

1. Introduction

1. This report presents the outcome of my Fault Studies & Severe Accident Analysis assessment of the BWRX-300 design as part of Step 2 of the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA). My assessment is based upon the information presented in the safety, security, safeguards and environment cases (SSSE) head document [1], specifically Chapters 1 to 10 (refs. [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]), Chapter 15 (ref. [13]) which contains 15.1 to 15.9 (refs. [14], [15], [16], [17], [18], [19], [20], [21], [22]), Chapters 22 (ref. [23]), Chapter 27 (ref. [24]), the associated revision of the Design Reference Report (DRR) (ref. [25]) and supporting documentation.

2. Assessment was undertaken in accordance with the requirements of ONR's Management System and follows ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [26]) and ONR's risk informed, targeted engagements (RITE) guidance (ref. [27]). The ONR Safety Assessment Principles (SAPs) (ref. [28]) together with supporting Technical Assessment Guides (TAGs) (ref. [29]), have been used as the basis for this assessment.

3. This is a Major report as per ONR's guidance on production of reports, NS-TAST-GD-108 (ref. [30]).

1.1. Background

4. The ONR's GDA process (ref. [31]) calls for an assessment of the RP's submissions with the assessments increasing in detail as the project progresses. This GDA will be finishing at Step 2 of the GDA process. For the purposes of the GDA, GE Vernova Hitachi Nuclear Energy International LLC, United Kingdom (UK) Branch, is the RP. GE Vernova Hitachi Nuclear Energy Americas LLC (GVHA) is a provider of advanced reactors and nuclear services and is the designer of the BWRX-300. GVHA is headquartered in Wilmington, North Carolina, United States of America (US).

5. In Step 1, and for the majority of Step 2, the RP was known as GE-Hitachi Nuclear Energy International LLC, UK Branch, and GVHA as GE-Hitachi Nuclear Energy Americas LLC. The entities formally changed names in October 2025 and July 2025 respectively. The majority of the submissions provided by the RP during GDA were produced prior to the name change, and thus the reference titles in Section 6 of this report reflects this.

6. In the UK, the RP is supported by its supply chain partner, Amentum, who has assisted the RP in the development of the UK-specific chapters of the Safety, Security, Safeguards and Environment cases (SSSE), and other technical documents for the GDA.

7. In January 2024, ONR, together with the Environment Agency and Natural Resources Wales, began Step 1 of this two-step GDA for the generic BWRX-300 design.

8. Step 1 is the preparatory part of the design assessment process and is mainly associated with initiation of the project and preparation for technical assessment in Step 2. Step 1 completed in December 2024. Step 2, which began in December 2024, is the first substantive technical assessment step, and will complete in December 2025.

9. The RP has stated that, at this time, it has no plans to undertake Step 3 of GDA and obtain a Design Acceptance Confirmation (DAC). It anticipates that any further assessment by the UK regulators of the BWRX-300 design will be on a site-specific basis and with a future licensee.

10. The focus of ONR's assessment in Step 2 was:

    - The fundamental adequacy of the design and safety, security and safeguards cases; and

    - The suitability of the methodologies, approaches, codes, standards and philosophies which form the building blocks for the design and cases.

11. The objective is to undertake an assessment of the design against regulatory expectations to identify any fundamental safety, security or safeguards shortfalls that could prevent ONR permissioning the construction of a power station based on the design.

12. Prior to the start of Step 2, I prepared a detailed Assessment Plan for Fault Studies and Severe Accident Analysis (ref. [32]). This has formed the basis of my assessment and was also shared with the RP to maximise openness and transparency.

13. This report is one of a series of assessments which support ONR's overall judgements at the end of Step 2 which are recorded in the Step 2 Summary Report (ref. [33]) and published on the regulators' website.

1.2. Scope

14. The assessment documented in this report is based upon the SSSE for the BWRX-300 (refs. [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48]).

15. The RP's GDA scope was agreed between the regulators and the RP during Step 1. This is documented in an overall Scope of Generic Design Assessment report (ref. [49]). This is further supported by its DRR (ref. [25]) and the Master Document Submission List (MDSL) (ref. [50]). The MDSL (ref. [50]) documents the submissions which were provided in each topic

area during Step 2 and provides a brief overview of the physical and functional scope of the nuclear power plant (NPP) that is proposed for consideration in the GDA. The DRR provides a list of the systems, structures and components (SSCs) which are included in the scope of the GDA, and its relevant GDA reference design documents.

16. The RP has stated it does not have any current plans to undertake GDA beyond Step 2. This has defined the boundaries of the GDA and therefore of my own assessment.

17. The GDA scope includes the Power Block (comprising the Reactor Building, Turbine Building, Control Building, Radwaste Building, Service Building, Reactor Auxiliary Structures) and Protected Areas (PA) as well as the balance of plant. It includes all modes of operation.

18. The regulatory conclusions from GDA apply to everything that is within the GDA scope. However, ONR does not assess everything within it or all matters to the same level of detail. This applies equally to my own assessment, and I have followed guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [26]) and ONR's guidance on Risk Informed, Targeted Engagements (ref. [27]).

19. As appropriate for Step 2 of the GDA, information has not been submitted for all aspects within the GDA Scope during Step 2. The following aspects of the SSSE are therefore out of scope of this assessment:

- The RP's fault analysis has not covered reactor start-up and shutdown operations including fuel handling above the reactor. Instead, the RP has provided a limited consideration of these operations and intends to cover with fault analysis in future. Unless otherwise stated, the conclusions of this report are limited to reactor and at power operations;
- The RP's fault analysis has excluded fault analysis of spent fuel storage; and
- The RP has not provided a completed identification of limits and conditions relating to operation, noting Step 2 GDA is focussed on identifying limits and conditions of the design (key design parameters).

20. Severe Accident Analysis (SAA) is within the scope of GDA. The RP made additional safety case submissions covering this topic during Step 2, although this is not reflected by the GDA scope report (ref. [49]). These submissions covered further information relating to severe accident methodology and deterministic analysis to demonstrate the effectiveness of identified safety features.

21. My assessment has considered the following aspects in line with my assessment plan (ref. [32]):

- Adequacy of the RP's approach to Defence in Depth, Safety Categorisation and Classification;
- Adequacy of the RP's approach to the deterministic analysis of faults within the design basis (DBA) and beyond the design basis (BDBA) including severe accidents;
- Identification of events and sequences;
- Effectiveness of the important and (in certain cases) novel systems for design basis and beyond design basis faults, including:
    - LOCA (Loss of Coolant Accident) protection provided by twin redundant Reactor Isolation Valves (RIVs);
    - nitrogen-inerted containment provision against releases from a LOCA;
    - natural cooling and RPV over-pressure protection provided by the triple redundant Isolation Condenser System (ICS);
    - general reliance on natural circulation as the single mode of core cooling;
    - general reliance on passive safety systems claiming independence from external sources of motive power or human intervention;
    - reactor protection systems provided by Control & Instrumentation (C&I); and
    - principal and alternative shutdown provisions.
- The RP's approach to severe accident analysis and feasibility of severe accident safety features;
- Approach to fault analysis of non-reactor faults, start-up and shutdown faults;
- The RP's consideration of radiological consequence assessment;
- Evidence for the validation of computer codes;
- The RP's approach to practical elimination of sequences with the potential for large or early release; and
- Enabling risks reduced ALARP.

2. Assessment standards and interfaces

22. The primary goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of the RP's SSSE for the reactor technology being assessed.

23. ONR has a range of internal guidance to enable Inspectors to undertake a proportionate and consistent assessment of such cases. This section identifies the standards which have been considered in this assessment. This section also identifies the key interfaces with other technical topic areas.

2.1. Standards

24. The ONR Safety Assessment Principles (SAPs) (ref. [28]) constitute the regulatory principles against which the RP's case is judged. Consequently, the SAPs are the basis for ONR's assessment and have therefore been used for the Step 2 assessment of the BWRX-300.

25. The International Atomic Energy Agency (IAEA) safety standards (ref. [51]) and nuclear security series (ref. [52]) are a cornerstone of the global nuclear safety and security regime. They provide a framework of fundamental principles, requirements and guidance. They are applicable, as relevant, throughout the entire lifetime of facilities and activities.

26. Furthermore, ONR is a member of the Western European Nuclear Regulators Association (WENRA). WENRA has developed Reference Levels (ref. [53]), which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors (ref. [54]).

27. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the TAGs (ref. [29]). The SAPs provide the principal means for assessing the Fault Studies & Severe Accident Analysis aspects.

28. The key guidance is identified below and referenced where appropriate within Section 4 of this report. Relevant good practice, where applicable, has also been cited within the body of this report.

2.1.1. Safety Assessment Principles (SAPs)

29. My judgements have been made against the 2014 Edition, Revision 1 (January 2020) version of ONR's SAPs (ref. [28]).

30. I have assessed against the following key SAPs:

- Fault Analysis FA.4 to FA.9 - For my assessment of design basis analysis. These guide my expectations related to the identification of initiating faults, demonstration that appropriate safety measures have

been identified, and measures are effective in mitigating fault consequences;

- Numerical Target NT.1 – I have also assessed against Target 4 of NT.1, which relates to mitigated radiological consequences for design basis faults;
- Fault Analysis FA.15, FA.16 and FA.25 - For my assessment of severe accident analysis aspects. These guide my expectations related to the identification of further reasonably practicable measures for severe accident management, and the demonstration of their effectiveness;
- Assurance of Validity AV.1 to AV.3, AV.5 and AV.6 - I have also considered the RP's assurance and validity of data and models. These relate to the validity of data and models, the provision of appropriate documentation, and the undertaking of sensitivity studies. I have not assessed against AV.4, AV.7 and AV.8, since these relate to matters largely outside of the control of RP;
- Key Engineering Principles EKP.3 to EKP.5 – These relate to application of defence in depth and the identification of safety functions and safety measures; and
- Safety Classification and Standards ECS.1 and ECS.2 – These relate to the categorisation of safety functions and classification of structures, systems and components (SSCs).

31. A list of the key SAPs used in this assessment is recorded in Appendix 1 – Relevant SAPs considered during the assessment.

2.1.2. Technical Assessment Guides (TAGs)

32. The following TAGs (ref. [29]) have been used as part of this assessment:

- NS-TAST-GD-005, Regulating duties to reduce risks ALARP
- NS-TAST-GD-006 (Rev 5), Design Basis Analysis
- NS-TAST-GD-007 (Rev 5), Severe Accident Analysis
- NS-TAST-GD-042 (Rev 5), Validation of Computer Codes and Calculation Methods
- NS-TAST-GD-051 (Rev 7), The purpose, scope and content of safety cases
- NS-TAST-GD-094 (Rev 2), Categorisation of Safety Functions and Classification of Structures, Systems and Components
- NS-TAST-GD-096, Guidance on Mechanics of Assessment

2.1.3. National and international standards and guidance

33. The following international standards and guidance have been used as part of this assessment:

- IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (ref. [55])
- IAEA, Deterministic safety analysis for nuclear power plants, Specific Safety Guide No. SSG-2 (ref. [56])
- IAEA, Design Extension Conditions and the Concept of Practical Elimination in the Design of Nuclear Power Plants No. SSG-88 (ref. [57])
- IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61 (ref. [58])
- WENRA Safety Reference Levels for Existing Reactor 2020 (ref. [53])
- WENRA Safety Objectives for New NPPs (ref. [54])

2.2. Integration with other assessment topics

34. To deliver the assessment scope described above I have worked closely with other topics to inform my assessment. Similarly, other assessors sought input from my assessment. These interactions are key to the success of GDA to prevent or mitigate any gaps, duplications or inconsistencies in ONR's assessment.

35. The key interactions with other topic areas were:

- Fuel and Core - to support my assessment of analytical methods supporting the RP's fault analysis and when considering adequacy of fuel performance acceptance criteria, safety margins and effectiveness of shutdown system(s);
- PSA - to support my assessment of the RP's severe accident analysis, the adequacy of severe accident safety features and consistency between the deterministic fault analysis and the PSA modelling;
- Structural integrity - when considering adequacy of acceptance criteria and safety margins concerning the integrity of the Reactor Coolant Pressure Boundary (RCPB) and suitability of safety classification;
- Other engineering topics - when considering the suitability of the safety classification and to gain confidence safety measures can deliver the safety functions required of them as assumed by the fault analysis (e.g. Electrical Engineering, Control and Instrumentation (C&I), Human Factors, Mechanical Engineering and Civil Engineering);

- Hazards - to gain confidence safety measures incorporate appropriate tolerance to Common Cause Failure (CCF) associated with hazards and that safety features address hazards associated with severe accidents; and

- Chemistry - to support my assessment of the RP's Severe Accident Analysis.

2.3. Use of technical support contractors

36. During Step 2 I have not engaged Technical Support Contractors (TSCs) to support my assessment of the Fault Studies and Severe Accident Analysis aspects of the GDA.

3. Requesting Party's submission

37. The RP submitted the SSSE at the start of Step 2 in four volumes that integrate environmental protection, safety, security, and safeguards. This was accompanied by a head document (ref. [1]), which presents the integrated GDA environmental, safety, security, and safeguards case for the BWRX-300 design.

38. All four volumes were subsequently consolidated to incorporate any commitments and clarifications identified in regulatory engagements, regulatory queries and regulatory observations, and were resubmitted in July 2025. This consolidated revision is the basis of the regulatory judgements reached in Step 2.

39. This section presents a summary of the RP's safety case for Fault Studies and Severe Accident Analysis. It also identifies the documents submitted by the RP which have formed the basis of my Step 2 assessment of the BWRX-300 design.

3.1. Summary of the BWRX-300 Design

40. The BWRX-300 is a single unit, direct-cycle, natural circulation, boiling water reactor with a power of ~870 MW (thermal) and a generating capacity of ~ 300 MW (electrical) and is designed to have an operational life of 60 years. The RP claims the design is at an advanced concept stage of development and is being further developed during the GDA in parallel with the RP's SSSE.

41. The BWRX-300 is the tenth generation of the boiling water reactor (BWR) designed by GVHA and its predecessor organisations. The BWRX-300 design builds upon technology and methodologies used in its earlier designs, including the Advanced Boiling Water Reactor (ABWR), Simplified Boiling Water Reactor (SBWR) and the Economic Simplified Boiling Water Reactor (ESBWR). The ABWR has been licensed, constructed and is currently in operation in Japan, and a UK version of the design was assessed in a previous GDA with a view to potential deployment at the Wylfa Newydd site. Neither the SBWR or ESBWR have been built or operated.

42. The BWRX-300 reactor core houses 240 fuel assemblies and 57 control rods inside a steel reactor pressure vessel (RPV). It uses fuel assemblies (GNF2) that are already currently widely used globally (ref. [5]).

43. The reactor is equipped with several supporting systems for normal operations and a range of safety measures are present in the design to provide cooling, control criticality and contain radioactivity under fault conditions. For post trip cooling, the BWRX-300's principal safety systems utilise natural circulation and passive cooling rather than active components, reflecting the RP's design philosophy.

44. The RP adopts the terminology of 'Anticipated Operational Occurrences' (AOOs), 'Design Basis Accidents' (DBAs) and 'Design Extension Conditions' (DECs). AOOs and DBAs are generally single events without fuel damage. DEC-A events involve multiple failures and may lead to limited fuel damage. DEC-B events are core damage scenarios.

45. The BWRX-300 reactor design provides the following key safety measures to support the fundamental safety functions (FSFs) 'core cooling', 'contain radioactivity' and 'control reactivity' during power operations:

- For AOOs and DBAs (all Class 1):
  - Isolation Condenser System (ICS)
  - Reactor and Containment Isolation Valves (RIVs and CIVs)
  - Primary Containment Cooling System (PCCS)
  - Scram[1] by hydraulic means of Control Rod (CR) insertion
  - Steel Plate Composite Containment Vessel (SCCV)
- For DEC-A events:
  - ICS, PCCS, SCCV, RIVs and CIVs as above
  - Reactor shutdown by motorised CR run-in (Class 2)

46. In the list above, RIVs/CIVs and PCCS are safety measures which are new to BWRX-300 compared with past BWR. All the measures support 'Defence Line' (DL) safety functions under the RP's safety strategy (Ref. [59]). The Defence Lines are fundamental to the RP's strategy and are described later in section 4.3.1. They reflect categories of safety function and broadly align with levels within the defence-in-depth (DID) hierarchy described in WENRA guidance for new reactors (ref. [54]) and in IAEA Safety Standards SSR2/1 (ref. [55]).

47. The PCCS is the only measure which is continuously available and relies solely on the natural movement of a working fluid. The others are available on demand by valves which actuate on loss of electrical power. These measures rely on a common set of C&I protection systems which monitor key reactor parameters and send de-energising trip signals to trigger valve actuation whenever limits are exceeded. The most significant C&I systems are:

- Anticipatory Protection System (APS) – Class 3

[1] The rapid shutdown of the reactor by insertion of control rods.

- Primary Protection System (PPS) – Class 1
- Diverse Protection System (DPS) – Class 2

48. The ICS provides the principal means of removing heat and therefore controlling reactor pressure during all faults, including intact circuit faults and loss of coolant accidents. The ICS is the only means of removing core decay heat following faults arising at power where the RPV is isolated from the main steam condenser. Heat is removed from the core and transferred to pools in a closed loop system. There are three trains of twin IC units (heat exchangers) submerged in pools within the Reactor Building (RB). Each IC unit comprises two drums joined by vertical tubes. Steam from the reactor enters the upper drum via a supply line before condensing within the tubes transferring heat to an ICS pool. Condensate then collects in the lower drum before returning to the RPV via a condensate return line. Figure 3 of Appendix 2 – Figures provides a diagram of the arrangement. The ICS pools provide the ultimate heat sink (UHS) by 'boiling off' to atmosphere.

49. The ICS is a Class 1 safety measure with three trains: A, B and C. Each train is held on standby and deployed by opening valves in the condensate return line. Once deployed, each train is designed to provide at least 72 hrs core cooling without the need for motive power or operator action. During deployment, radiolytic gases can form in the ICS which could potentially affect performance. The ICS units have key features against the build-up of radiolytic gas (see section 6.2.1.1 of ref. [7]). Radiolytic gases are purged via a vent line during normal operation which is automatically isolated by spring loaded valves which close whenever the unit is put in duty. Each unit also has integral passive catalytic recombiners to purge gases during deployment (i.e. during accident conditions).

50. Since the ICS is a closed loop system, any significant pipe breaks that would challenge its safety function need to be isolated. Reactor Isolation Valves (RIVs) are included in the design near the reactor connection point of any large pipework. The RIVs are provided in redundant pairs and are designed to close within 10 seconds to arrest the loss of reactor coolant and preserve the inventory.

51. The Primary Containment System (PCS) acts as the final barrier to release of radioactivity to the environment during accident conditions. It comprises:

- RIVs – as well as preserving RPV inventory, the RIVs also provide a role in containment of radioactivity;

- CIVs - which are located on all reactor coolant pipework both inboard and outboard[2] of the containment penetrations. Where the pipework already contains RIVs, these act as the inboard containment isolation; and

- SCCV - the SCCV forms the physical barrier for containment safety functions. It also includes support structures for the Nuclear Boiler System (NBS) comprising the RPV and its connecting pipes. This contains a nitrogen inert atmosphere and has no compartments (see section 6.5.2.3 of ref. [7]).

52. Aside from the RIVs on the ICS pipework, both the RIVs and CIVs are designed to close either on loss of power supplies or on initiation by the PPS or DPS. The RIVs on the ICS pipework are only initiated to close via the PPS to avoid the possibility of spurious actuation by the DPS. The RIVs on the ICS pipework can also be closed manually via the secondary control room (SCR).

53. During large loss of coolant accidents (including steam line breaks), prior to isolation via the RIVs, a finite mass and energy release into the SCCV occurs. In these scenarios, the PCCS is designed to protect the SCCV from excessive pressure and temperature. The PCCS also removes heat from the containment during smaller unisolable loss of coolant accidents. However, in both accidents, it plays no significant role in decay heat removal. Cool water from the equipment pool outside of containment flows through the PCCS pipework, removing heat from the containment, and the warmer water is returned to the equipment pool. A diagram is provided in Figure 4 of Appendix 2 – Figures. The RP also claims that significant heat is naturally transferred via the containment closure head above the RPV to the reactor cavity pool. The RP claims that due to the limited energy release from the break, and the other natural losses, the bulk temperature of the equipment pool does not reach boiling temperature and does not require makeup to fulfil its safety function during the mission time for any design basis fault. The PCCS, the closure head and the SCCV are all Class 1.

54. Table 1 summarises how the ICS and the PCS protect against faults and support FSFs.

[2] Throughout this Assessment Report, I refer to “inboard” and “outboard” to describe a location of valves relative to the RPV. Inboard RIVs refers to valves that are closer to the RPV, whilst outboard RIVs refers to those further down a pipe, away from the RPV. Inboard and outboard CIVs refers to valves on the inside and outside of the containment, respectively.

Table 1 : Summary of Safety Measures

Safety Measure	Fundamental Safety Functions (FSFs)	
	Core Cooling	Contain Radioactivity
ICS	Cools the core following a reactor trip	Protects the RPV from over-pressure following an intact circuit reactor fault
PCS	Preserves coolant inventory following LOCAs[3]	Contains or limits radioactive release following LOCAs

55. Hydraulic Scram provides the principal means of safe reactor trip and shutdown following all reactor faults and is delivered by Hydraulic Control Units (HCUs) via the following 'fail-safe' means:

- Pneumatic Scram valves which spring open whenever the Scram solenoids on the actuating lines are de-energised by trip signals from any of the three C&I protection systems or by the manual switches in the Main or Secondary Control Rooms (MCR or SCR); and
- Independent Alternative Rod Insertion (ARI) valves which also spring open following any trip signal.

56. Motorised Control Rod (CR) run-in provides a secondary means of safe shutdown (Class 2) for DEC-A sequences where the principal means (Hydraulic Scram) fails. This operates independently of the Hydraulic Scram and is simultaneously tripped by any of the C&I protection systems. The PPS incorporates design features which isolates it from faults arising within any of the lower-class systems that it triggers.

57. BWRX-300 provides the following features to defend against containment failure during DEC-B core melt scenarios and to prevent a large or early release of radioactivity:

- The UPR (Ultimate Pressure Regulator) is designed to reduce RPV pressure to prevent high pressure melt ejection (HPME) and direct containment heating (DCH) phenomena;

[3] Large LOCAs are isolated by the RIVs which both preserve coolant inventory and arrest the discharge. For small unisolable LOCAs the PCCS helps depress containment pressure below RPV pressure and avoid nitrogen ingestion.

- The corium shield is designed to prevent direct contact between a relocated molten core and the concrete basemat plus other parts of the containment structure (Molten Core Concrete Interaction);
- The containment vent prevents over-pressurising the containment; and
- Nitrogen-inerted containment prevents hydrogen deflagrations within containment.

58. Further information on these features is provided in section 4.3.5.3.

59. The Boron Injection System (BIS) provides a further independent alternative means of safe shutdown (Class 3) in DEC scenarios where rod insertion has failed. The RP has clarified that the effectiveness of the BIS in these circumstances relies on the ICS, the UPR (Ultimate Pressure Regulator) plus the containment vent to control pressure and reactivity while it is being deployed (see section 4.3.10.3 for detail).

3.2. BWRX-300 Case Approach and Structure

60. The RP has submitted information on its strategy and intentions regarding the development of the SSSE (refs [59], [60], [61], [62]). This was submitted to ONR during Step 1.

61. The RP has submitted a SSSE for the BWRX-300 that claims to demonstrate that the standard BWRX-300 can be constructed, operated, and decommissioned on a generic site in GB such that a future licensee will be able to fulfil its legal duties for activities to be safe, secure and will protect people and the environment. The SSSE comprises a Preliminary Safety Report (PSR) which also includes information on its approach to safeguards and security, a security assessment, and a Preliminary Environment Report (PER), and their supporting documents.

62. The format and structure of the PSR largely aligns with the IAEA guidance for safety cases, SSG-61 (ref. [58]), supplemented to include UK specific chapters such as Structural Integrity and Chemistry. The RP has also provided a chapter on As Low as Reasonably Practicable (ALARP), which is applicable to all safety chapters. The RP has stated that the design and analysis referenced in the PSR is consistent with the March 2024 Preliminary Safety Analysis Report (PSAR) submitted to the US Nuclear Regulatory Commission (NRC). The Security Assessment and PER are for the same March 2024 design but have more limited links to any US or Canadian submissions.

3.3. Summary of the RP's case for Fault Studies and Severe Accident Analysis

63. Table 5-2 of the RP's GDA Safety Case Development Strategy (ref. [62]) provides a complete list of the safety case claims. These claims are arranged into 3 levels, topped by an overall claim:

    Overall Claim - 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.

64. There are four claims underpinning the overall claim. Of those claims, my assessment of Fault Studies and Severe Accident Analysis relates to claim 2 and the selection of claims falling beneath:

    - Claim 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):
        - Claim 2.1 – The functions of systems and structures have been derived and substantiated taking into account RGP and OPEX, and processes are in place to maintain these through-life. (Engineering Analysis);
        - Claim 2.3 – A suitable and sufficient safety analysis has been undertaken which presents a comprehensive fault and hazard analysis that specifies the requirements on the safety measures and informs emergency arrangements. (Safety Analysis); and
        - Claim 2.4 -Safety risks have been reduced as low as reasonably practicable.

65. Under Claim 2.1, the RP claims that a robust analysis, based on RGP (Relevant Good Practice) has been used to derive the safety functions for the system/structure. This claim is supported by evidence presented in Chapter 3 of the PSR (ref. [4]) covering safety objectives and design rules, and by Chapter 15 of the PSR covering safety analysis (refs [14], [15], [16], [17], [18], [19], [20], [21], [22]).

66. Claim 2.3 concerns the adequacy of the safety analysis and is therefore of greatest relevance to my assessment along with the evidence concerning the fault analysis presented in Chapters 15.2 (ref. [15]), 15.3 (ref. [16]) and 15.5 (ref. [18]). The following sub-sections therefore focus on Claim 2.3 in more detail.

3.3.1. Identification and Assessment of Initiating Events

67. In support of claim 2.3, the RP claims within the SSSE that a systematic approach has been used to identify postulated initiating events (PIEs) and they have been categorised, grouped and assessed appropriately. The evidence for this is largely presented in Chapter 15.2 (ref. [15]).

3.3.2. Design Basis Events Appropriately Assessed

68. In support of claim 2.3, the RP claims within the SSSE that an appropriate subset of grouped events has been derived and subjected to deterministic analysis. The RP claims this analysis has been conservatively performed using appropriately validated and verified analytical models to appropriate acceptance criteria and targets. The RP claims that its fault analysis:

- Demonstrates the effectiveness of safety measures;
- Demonstrates that small changes in fault severity do not lead to cliff-edge increases in consequence;
- Provides a clear, auditable linkage between PIEs, sequences and safety measures;
- Enables identification of limits and conditions; and
- Enables adequate categorisation of safety functions and classification of SSCs.

69. The evidence underpinning the above is largely presented in Chapter 15.5 (ref. [18]) and its supporting references. This includes evidence which covers the use of the fault analysis to inform the RP's safety classification approach. This is described in BWRX-300 SSC Safety Classification Report (ref. [63]).

3.3.3. Beyond Design Basis and Severe Accidents Appropriately Assessed

70. In support of claim 2.3, the RP claims within the SSSE that a systematic approach has been used to analyse beyond design basis states, focussing on how the accident state or scenario will be controlled and/or mitigated.

3.3.4. ALARP by Design

71. In support of claim 2.4, the RP makes claims within the SSSE that the design will enable risks to be demonstrated to be reduced ALARP by applying the following:

- Relevant Good Practice (RGP) across all disciplines
- Operational Experience (OPEX) and Learning from Experience (LfE)
- Optioneering

- Comparison of residual risks against targets

3.4. Basis of assessment: RP's documentation

72. The principal documents that have formed the basis of my Fault Studies and Severe Accident Analysis assessment of the SSSE are:

    - Chapter 3 of the PSR (ref. [4]) which describes the safety objectives and design rules for SSCs;
    - BWRX-300 Safety Strategy Specification (ref. [59]) which sets out the fault analysis approach and the rules for the deterministic fault analysis;
    - Chapter 15.2 of the PSR (ref. [15]) which describes how events have been categorized and grouped for deterministic fault analysis;
    - Chapter 15.3 of the PSR (ref. [16]), which describes the safety objectives and acceptance criteria for the deterministic fault analysis;
    - Chapter 15.5 of the PSR (ref. [18]) which describes the deterministic fault analysis which has been applied to the groups; and
    - Chapter 27 of the PSR (ref. [24]) which describes the approach to ALARP evaluation.

73. Whilst Chapter 3 (ref. [4]) sets out the safety objectives and rules, my assessment has focused on the lower-tier documents that support this chapter and Chapter 15, in which these objectives and rules are implemented.

3.5. Design Maturity

74. My assessment is based on revision 3 of the DRR (ref. [25]). The DRR presents the baseline design for GDA Step 2, outlining the physical system descriptions and requirements that form the design at that point in time.

75. The reactor building and the turbine building, along with most of the significant structures, systems and components (SSCs) are housed within the 'power block'. The power block also includes the radwaste building, the control building and a plant services building. For security, this also includes the PA boundary and the PA access building.

76. The GDA Scope Report (ref. [49]) describes the RP's design process that extends from baseline BL0 (where functional requirements are defined) up to BL3 (where the design is ready for construction).

77. In the March 2024 design reference, SSCs in the power block are stated to be at BL1. BL1 is defined as:

- System interfaces established;
- (included) in an integrated 3D model;
- Instrumentation and control aspects have been modelled;
- Deterministic and probabilistic fault analysis has been undertaken; and
- System descriptions developed for the primary systems.

78. The balance of plant remains at BL0 for which only plant requirements have been established, and SSC design remains at a high concept level.

79. It is fundamental to the RP's safety strategy (ref. [59]) that the fault analysis is developed in tandem with the maturing design and is first applied at BL1. For GDA Step 2 this means the fault analysis is limited to covering the 'power block', which contains the most safety important and novel safety measures.

4. ONR assessment

4.1. Assessment Strategy

80. The objective of my GDA Step 2 assessment was to reach an independent regulatory judgement on the fundamental aspects of the BWRX-300 design relevant to Fault Studies & Severe Accident Analysis as described in Sections 1 and 3 of this report. My assessment strategy is set out in this section and defines how I have chosen which matters to target for assessment. My assessment is consistent with the delivery strategy for the BWRX-300 GDA (ref. [64]).

81. GVHA is currently engaging with regulators internationally, US NRC and the Canadian Nuclear Safety Commission in Canada (CNSC). It is proposing a standard BWRX-300 design for global deployment with minimal design variations from country to country. My assessment takes cognisance of work undertaken by overseas regulators where appropriate. I have taken credit for their reviews of the RP's fault analysis where our regulatory guidance and standards are comparable.

82. Whilst there is no operating BWR plant in the UK, ONR has previously performed a full GDA on the Hitachi-GE UK ABWR (ref. [65]). I have taken learning from this previous activity, targeting my assessment on those aspects of the BWRX-300 which are novel or specific to this design. I have not looked to reassess inherent aspects of BWR technology which were considered in significant detail for the UK ABWR and judged to be adequate.

83. My assessment has followed my Assessment Plan (ref. [32]). My assessment has targeted the following areas:

- Adequacy of approach and implementation of Defence in Depth, Safety Categorisation and Classification (Section 4.3.1);
- Fault analysis approach to design basis and beyond design basis events (Section 4.3.2);
- Identification of faults and event sequences (Section 4.3.3);
- Effectiveness of design basis safety measures (Section 4.3.4);
- Approach to severe accident analysis and feasibility of severe accident safety features (Section 4.3.5);
- The RP's approach to fault analysis of non-reactor faults, start-up and shutdown faults (Section 4.3.6);
- The RP's consideration of radiological consequence assessment (Section 4.3.7);

- Evidence of validation of computer codes (Section 4.3.8);
- The RP's approach to practical elimination of sequences with the potential to lead to large or early release (Section 4.3.9); and
- Enabling risks reduced ALARP (Section 4.3.10).

84. In Section 4.3, I have structured my report around the above targeted matters.

85. In addition, I have also summarised my assessment of the safety case documentation in Section 4.3.11.

4.2. Assessment Scope

86. My assessment scope and the areas I have chosen to sample for my assessment are set out in this section.

87. My assessment scope is consistent with the GDA scope agreed between the regulators and the RP during Step 1 and detailed in Section 1.2 of this report. I have targeted my assessment within this scope.

88. In line with the objectives for Step 2, I have undertaken a broad review of the highest level, fundamental claims and supporting arguments related to Fault Studies & Severe Accident Analysis. To support this, I have sampled a targeted set of the claims or arguments as set out below. Where applicable, I have also sampled the evidence available to support any claims and arguments.

89. To carry out my assessment of the above targeted matters, it has been necessary to sample the safety case with both a system based and fault-based view.

90. As per my targeted matters, I have focussed my assessment on defence in depth levels 3 and 4, as described in ONR's SAPs (ref. [28]). My assessment has, therefore, focussed on the most safety significant safety measures claimed for these levels. Since limited information was available regarding severe accident analysis, I have taken a high-level approach to my assessment of severe accident safety features. I have focussed my assessment on the following safety measures of the BWRX-300:

- ICS
- PCS (including RIVs, CIVs and PCCS)
- Hydraulic Scram
- Scram by motorised CR run-in
- Severe accident safety features

91. With a fault-based view, and aligned with my assessment plan (ref. [32]), I have sampled the following faults/scenarios:

- Large break LOCAs within containment - these put greatest demand on the RIVs and PCCS, and mission time of the ICS. The RIVs are required to close rapidly to retain sufficient coolant inventory to maintain a water level above the core and to enable ICS decay heat removal. LOCAs also pose a challenge for the mission time of the ICS, since one train is potentially lost through a break in ICS pipework. The PCCS is required to remove heat from the containment during the mass and energy release from the break. In both aspects, the large break LOCA is bounding of all other faults;

- Small break LOCAs within containment - These may remain un-isolated and place additional longer term demands on the performance of both the ICS and PCCS, as well as introducing challenges related to nitrogen ingress (see Appendix 3 – Findings by other regulators);

- Overpressure faults – these faults, such as sudden interruption of the main steam flow, result in a rapid pressure increase and void collapse in the RPV, leading to a rapid reactivity insertion. Besides control rod withdrawal or drop faults (see paragraph 92 below), these faults are bounding for ICS and reactor scram performance. In addition, unlike other faults in which heat continues to be removed by the steam system until RIV isolation, these faults, by their nature, result in a rapid loss of duty heat sink. This makes the core conditions more onerous than for any other intact circuit fault; and

- Severe accidents – these may introduce phenomena which place demand on further safety features to defend the containment and mitigate release.

92. In formulating my sampling strategy, I considered other general challenges for the BWR, including density wave oscillations and control rod withdrawal or drop faults. I judge these aspects are covered by ONR's GDA of ABWR (ref. [66]) and/or in more detail in the ONR Fuel and Core assessment of BWRX-300 (ref. [67]) and have therefore excluded these from my sample. My reasoning can be summarised as follows:

- Density-wave oscillations - loss of feedwater heating events can lead to reactivity and thermal hydraulic instability. This is a unique challenge for BWR caused by the voidage in the core channels[4]. However, compared

[4] Feedwater pre-heating keeps core inlet temperatures close to saturation to optimise heat transfer rates from the fuel and reactor performance. Any loss in heating leads to sub-cooled water entering the core inlet which reduces voidage. There is an initial reactivity insertion as local

to the ABWR, BWRX-300 is more stable due to its naturally responsive flow rates and the orifices in its core support plate which lessen the impact of void changes on flow. Moreover, the BWRX-300 provides a select control rod run-in (SCCRI) measure to control the phenomenon. This can stabilise the reactor at lower power and avoid a scram; and

- Other reactivity faults which are unique to a BWR involve control rod drop out of the core. However, along with control rod withdrawal faults, I consider these to be covered by GDA of ABWR since they are similarly defended by the Fine Motion Control Rod Drive (FMCRD) design and its key features which have been previously assessed (ref. [66]).

93. For severe accident analysis, I have not assessed the deterministic analysis to the same degree as for the DSA covering DBAs and DEC-A sequences. This is because the PSR which was submitted for assessment at the start of Step 2 GDA provided limited information. Severe accident safety features were described to be in concept and no analysis was submitted. Analysis was later formally submitted as supplementary information during Step 2 (in response to an RQ raised during Step 1). So instead, I have assessed whether the appropriate phenomena are identified, appropriate safety features are identified to prevent or mitigate those phenomena, and that the design concepts have been developed and demonstrated effective at high level.

94. For non-reactor faults and faults during start-up and shutdown, the RP has not presented any deterministic analysis. However, I have been able to sample a fuel drop scenario and a loss of shutdown cooling scenario where the RP has made some consideration of the consequences in order to gain confidence in the RP's approach.

4.3. Assessment

4.3.1. Approach to Defence in Depth, Safety Categorisation and Classification

95. For BWRX-300, defence in depth is based on layers of physical barriers to radioactive release defended by implemented safety requirements. The RP's safety strategy (ref. [59]) describes how these requirements are organised into a hierarchy of Defence Lines (DLs) depending on objectives (see Figure 1). I am content that these DLs and their objectives are set out in adequate detail in Chapter 3 of the PSR (ref. [4]). It is important to note that DLs are not the physical barriers comprising fuel clad, reactor coolant pressure boundary and containment. DLs are a concept for marshalling the safety

coolant density increases improving moderation. However, as the denser region moves up through the core, it imposes a higher flow resistance reducing flow upstream. The lower flow results in increased coolant temperatures and voidage, reducing reactivity. The delay between the initial insertion of reactivity and subsequent withdrawal causes oscillations.

features, functions and operational practices into a hierarchy of levels which protect the integrity of the physical barriers and broadly align to the defence-in-depth hierarchy described in EKP.3 of the SAPs (ref. [28]), in IAEA Safety Standards SSR2/1 (ref. [55]) and in Appendix 1 of WENRA Applicability of Safety Objectives to SMRs (ref. [54]).

Defense Line	Objective
DL1	Minimize potential for failures and initiating events to occur in the first place and minimize potential for failures to occur in subsequent lines of defense.
DL2	Actively control key plant parameters associated with FSFs, and detect and mitigate AOO PIEs.
DL3	Detect and mitigate DBA PIEs and event sequences comprising AOO PIEs and failure of DL2 functions.
DL4a	Detect and mitigate DECs, including event sequences associated with some DBA PIEs and failure of DL3 functions.
DL4b	Detect and mitigate DECs to prevent core damage or mitigate the consequences of core damage events (severe accidents).

Figure 1: Overview of Defence Line Objectives (Source of content - ref. [59])[5]

96. The key design basis safety measures targeted by my assessment are described in section 3.1 along with the severe accident features. The following DLs are of greatest interest and are supported by those measures and features as follows:

- DL3 by the ICS, RIVs and CIVs, PCCS, PPS and Hydraulic Scram. These measures provide the principal means of protecting the reactor in design basis events;
- DL4a by the DPS and Scram by motorised Control Rod (CR) run-in. These measures act as diverse ‘back-ups’ to the PPS and Hydraulic Scram respectively; and
- DL4b by the BIS and severe accident features which include UPR, corium shield and containment vent.

97. The RP has consistently chosen to use DL2 for the control functions against abnormal occurrences, DL3 for the principal safety functions of protection

[5] A further DL5 is also defined covering emergency preparedness measures for protecting the public from consequences of release of radioactive materials.

against design basis events and DL4a for the 'back-up' functions. This means DL levels 2 to 4 directly correlate to the safety categorisation of those allocated safety functions and the safety class of the SSCs supporting them. The RP regard this correlation between the DL levels 2 to 4, safety categories and safety class to be a fundamental aspect of the BWRX-300 safety strategy, which I consider further below.

4.3.1.1. Categorisation of Safety Functions and Classification of SSCs

98. It is my expectation that safety functions and the SSCs which deliver them, are identified then categorised and classified as appropriate to reflect their safety significance. It is also my expectation that the deterministic analysis is used to inform this process. It is my expectation that this is applied to all safety functions and SSCs that support all modes of operation. My expectations are informed by EKP.4, EKP.5, ECS.1, ECS.2 and FA.9 of the SAPs (ref. [28]) and NS-TAST-GD-094 (ref. [68]) and IAEA's SSG-30 (ref. [69]).

99. In ref. [70], the RP has systematically derived safety functions and assigned SSCs to perform those functions. There is a clear link between the safety functions and the SSCs that perform them, meeting my expectations informed by EKP.4 and EKP.5 of the SAPs (ref. [28]).

100. The RP's approach to categorisation and classification of safety functions and SSCs is described in ref. [63]. This approach covers reactor faults and can be summarised as follows:

- The deterministic analysis of reactor faults and event sequences is used to determine plant specific safety functions and assign them to a DL level based on their safety objective within the DL hierarchy and their importance in securing FSFs for the event sequence;
- Each DL level is then assigned a safety category (1,2,3 or N), where category 1 is the highest safety significance, as follows:
    - DL2 - safety category 3 or N
    - DL3 - safety category 1
    - DL4a - safety category 2
    - DL4b - safety category 3 or N
- If a DL function is not needed until after 72hrs post event, then it may drop to a lesser safety category;
- The SSCs which deliver the DL functions (or support their delivery) are classed at the same level as the highest safety category of DL function they deliver (or support). For example, an SSC which delivers (or

supports) a DL3 function will be safety class 1 whatever other lower category DL functions it may deliver (or support); and

- Apart from the PCCS, the SSCs which concern the DL3 and DL4 functions are held on 'standby'. These require supporting SSCs to operate continuously and maintain them in a state of readiness for deployment during events. While required under normal conditions those SSCs are not required to fulfil the mission during fault conditions. An example would be SSCs which maintain the initial temperatures of the IC pools within limits. These SSCs are classed at a lower level than the SSCs that they 'make-ready'.

101. Ref. [15] lists the integrity targets for each DL, reflecting its safety category. The RP's 'Fault Evaluation' document (ref. [70]) places reliability requirements on supporting SSCs to ensure they have adequate independence, are available on demand and perform with the reliability required to support these targets:

- $1x10^{-2}$ failure/demand for DL2 (as delivered by APS)
- $1x10^{-4}$ failure/demand for DL3 (as delivered by ICS, PCS and PPS)
- $1x10^{-3}$ failure/demand for DL4a (as delivered by DPS)

102. ONR's expectations for categorisation and classification are not aligned to levels of defence in depth in the same way as the RP's. However, NS-TAST-GD-094 (ref. [68]) explains that for complex facilities, such as a reactor, it is appropriate to place the highest reliability claims (Class 1) on Level 3 defence-in-depth. Moreover, it is common practice for reactors to do so, and to classify the back-up safety measure (also Level 3) as Class 2 and severe accident safety features (Level 4) as Class 3.

103. With regards to modifications of categorisation and classification following a period after an accident and the lower classification of supporting systems not required during the deployment of the safety function, these too are commonly applied (see ref. [71]), and align with the expectations set out in NS-TAST-GD-094 (ref. [68]) and SSG-30 (ref. [69]).

104. For Overpressure faults and LOCAs the principle means of protection is the PCS, ICS and Hydraulic Scram. These are therefore assigned Class 1. The back-up means of initiation of PCS, ICS and Hydraulic Scram is Class 2. There are no alternative routes for heat removal to the PCS and ICS (see section 3.1). However, the back-up motorised CR run-in for alternative shutdown is assigned Class 2. Severe accident mitigation for both faults is Class 3. Based on guidance provided in NS-TAST-GD-094 [68] and IAEA's SSG-30 (ref. [69]), I judge that this is appropriate.

105. For shutdown and 'non-reactor' operations, the RP has not applied an approach to categorisation and classification. As informed by ECS.1 and

ECS.2 of the SAPs (ref. [28]), I expect that the categorisation and classification be applied to all safety functions and SSCs for all modes of operation. I, therefore, judge that this is a gap against my expectations. The RP has identified this gap in a review undertaken against UK expectations (ref. [72]) and has committed to developing its approach to categorisation and classification in support of a future submission. Based on the RP's 'gap review' (ref. [72]) and the adequate approach taken for reactor power operations, I am content that an adequate safety case can be made in the future.

106. Overall, I am therefore satisfied that RP's approach to categorisation of safety functions and classification of SSCs for power operation of the reactor meets my expectations for EKP.4, EKP.5, ECS.1, ECS.2 and FA.9 (ref. [28]), NS-TAST-GD-094 (ref. [68]) and SSG-30 (ref. [69]). However, a future safety case would need to demonstrate an adequate categorisation and classification approach applied to shutdown and non-reactor operations.

4.3.1.2. Defence in Depth

Informed by EKP.3 of the SAPs (ref. [28]), it is my expectation that the principle of defence in depth is applied, and that each level is adequately independent from each other, to avoid common cause failures across multiple levels. In addition, I also expect, informed by ERC.2 of the SAPs (ref. [28]), that two independent means of shutting down the reactor are provided. SAP EDR.3 (ref. [28]) also sets expectations related to reasonable limitations to reliability claims[6] which I note typically results in two lines of protection being expected for more frequent faults.

107. The RP claims that the BWRX-300 defence-in-depth concept ensures the following levels of independence amongst Defence Lines (see section 2.1.3 of ref. [59]). Note the RP uses the word 'mitigate' to mean achieving the objective against the criteria applied at that level[7]:

- Amongst DLs 2, 3 and 4, two independent and diverse lines can mitigate any initiating event with a frequency greater than $1x10^{-5}$ pa, for events caused by single failures; and
- Amongst DLs 2, 3 and 4, at least one line can mitigate any initiating event caused by a common cause failure (CCF) in another DL, with the mitigation means being independent from the effects of the initiating CCF.

[6] EDR.3 of SAPs (ref. [28]) gives a figure of one failure per 100 000 demands as the best value for a simple system

[7] DLs 2,3 and 4a all protect the core from damage with varying safety margin while DL4b protects against the consequences of core damage

108. As explained in NS-TAST-GD-006 (ref. [29]), and based on RGP from other reactor designs, I would typically expect a second line which is clearly independent and diverse from the first to be identified for frequent faults. For the BWRX-300 though, I note that two lines (DL3 and DL4a) both ultimately rely on passive cooling using the ICS. This implies a very high reliability claim on the ICS against CCF which could challenge my expectations of what is reasonably supportable and my expectations of a diverse safety measure for frequent faults. However, this does depend on how well underpinned the reliability of the principal means of protection is. I consider the underpinning of the ICS later in the identification of sequences section (see section 4.3.3) where, based on my findings, I judge that a high reliability claim is supportable. I do not therefore consider the lack of deterministic claims on a diverse heat removal system necessarily implies a fundamental safety shortfall against my expectations for defence in depth. However, I do consider it warrants further assessment for a future safety case.

109. Aside from the above matters, both the principal and alternative means of shutdown commonly rely on insertion of shutdown rods. In my opinion, this presents a potential shortfall against my expectations for independence of levels of defence in depth and diverse means of shutdown, as informed by EKP.3, and ERC.2 of the SAPs (ref. [28]). Moreover, it is a potential shortfall against Requirement 46 of SSR-2/1 (ref. [55]). I revisit this topic in the identification of sequences section (see section 4.3.3) and in the ALARP section (see section 4.3.10) where I take confidence from additional evidence provided by the RP that a suitably diverse measure based on BIS can close any gap for a future safety case.

110. Both the above potential shortfalls concern the adequacy of independence of two levels of defence in depth (DL3 and DL4a) which I consider in more detail in section 4.3.3, where confidence in the common ICS and Scram means is forthcoming. In the meantime, at high level I consider that the RP's general approach to applying the defence in depth concept and seeking multiple independent barriers to fault progression is in keeping with EKP.3 of the SAPs (ref. [28]).

4.3.2. Approach to Fault Analysis

111. This section summarises my assessment of the RP's approach to fault analysis mainly set down in the RP's safety strategy (ref. [59]) and Chapter 15.2 of the PSR (ref. [15]). This covers the general approach to fault analysis covering DBAs/DEC-A. A more detailed summary of my assessment of each area can be found in subsequent sections. Section 4.3.3 covers the identification of DBAs/DEC-A while section 4.3.4 covers effectiveness of DBAs/DEC-A safety measures. Note that severe accident analysis (DEC-B) is all covered in section 4.3.5.

112. In general, it is my expectation that conservative deterministic analysis is performed to demonstrate safety measures to be effective against design basis faults and that radiological targets are met. To identify those faults, I

expect initiating events to be identified and grouped, and sequences developed which consider the failure of safety measures. I expect a fault schedule to be constructed which links the initiating events to the protective safety measures and that limits and conditions of the plant are derived from the analysis. In addition, I expect that beyond design basis and severe accident sequences are analysed, and that safety features are provided to mitigate the consequences. These expectations are informed by NT.1, FA.1-9, FA.15 & FA.16 of ONR SAPs (ref. [28]), NS-TAST-GD-006 and NS-TAST-GD-007 (ref. [29]), SSR-2/1 (ref. [55]) and SSG-2 (ref. [56]).

4.3.2.1. Fault identification and categorisation

113. The RP applies hazard identification techniques to identify initiating events in all modes of operation. This is covered further in section 4.3.3.

114. The RP's methodology, which it terms 'Fault Evaluation', groups initiating events into PIEs[8]. It uses a best estimate approach for initiating event frequency and assumes that any events which could challenge FSFs could lead to potential core damage. The RP categorises these events according to frequency using the terminology 'AOO Event Sequences', 'DBA Event Sequences' and 'DEC Event Sequences' (see Figure 2 below). AOOs and DBAs cover all potential core damage events which have a frequency greater than $1x10^{-5}$ pa.

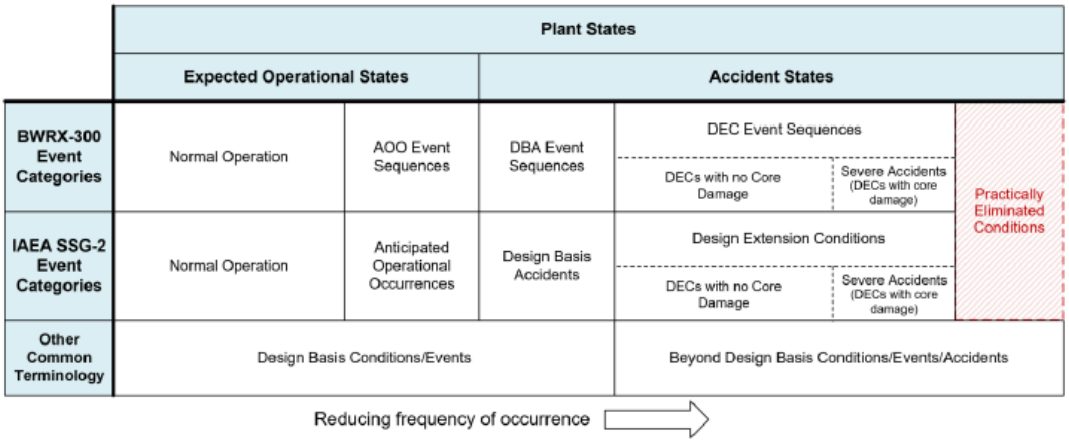

Figure 2: Plant States and Event Categories (Source of content - ref. [59])

115. Although the RP has not presented unmitigated consequences for the DBA sequences, I judge that a conservative assumption of core damage is sufficient for the identification of faults that should be treated within the design basis. This, coupled with the criteria for inclusion of design basis accidents with a frequency of greater than $1x10^{-5}$ pa, meets my expectations

[8] Figure 3-1 of ref. [59] illustrates the RP's fault analysis approach with box 4 covering 'Fault Evaluation'

for the inclusion of faults within the design basis, aligned with SAP FA.5 (ref. [28]).

116. The RP's 'Fault Evaluation' (ref. [70]) is the RP's systematic process for deriving event sequences from PIEs and categorising those event sequences into AOO, DBA or DEC depending on their frequency:

- AOO – sequences with frequency greater than $1x10^{-2}$ pa
- DBA – sequences with frequency between $1x10^{-2}$ and $1x10^{-5}$ pa
- DEC-A – sequences with limited fuel failure (either initiating event frequencies are less than $1x10^{-5}$ pa, or sequences involve multiple failures)
- DEC-B – sequences with core damage (no associated frequency)

117. For AOOs, DBAs and DEC-A sequences, the sequences are then grouped and bounded for a graded level of deterministic safety analysis (DSA)[9]. ONR's SAPs (ref. [28]) set the expectation that sequences are analysed down to 10^{-7} pa using design basis techniques, and that sequences that lie just beyond the design basis initiating event cut-off frequency are analysed. As described in NS-TAST-GD-006 (ref. [29]), this often manifests in identifying diverse lines of protection for frequent faults. The RP's approach aligns with the approaches described in WENRA guidance (ref. [54]) and IAEA's SSR-2/1 (ref. [55]). This appears more granulated than the approach described in the SAPs (ref. [28]) which simply consider fault sequences that lie within design basis and beyond design basis (as illustrated in Figure 2). I consider the RP's approach to deriving and categorising event sequences to be in keeping with my expectations for identifying initiating events and sequences against SAPs FA.5 and FA.6 (ref. [28]), and my expectations for design extension conditions as derived from IAEA's SSR-2/1 (ref. [55]).

4.3.2.2. Approach to deterministic analysis

118. AOOs are analysed to determine the expected plant response and performance of control functions within DL2, referred to by the RP as 'BL-DSA'. Since my assessment has targeted DL3 and DL4, protection of AOOs afforded by DL2 has not fallen within my sample. However, although I have not assessed the deterministic analysis in any detail, I note this approach provides additional confidence in the robustness of DL2 and overall demonstration of defence-in-depth.

119. DBAs are analysed in a conservative manner, referred to by the RP as 'CN-DSA', to determine the performance of the protective safety functions within DL3 and demonstrate their effectiveness. Important parameters are

[9] The grades of DSA are denoted BL-DSA, CN-DSA and EX-DSA and are applied to AOOs, DBAs and DECs respectively (represented in box 6 of Figure 3-1 of ref. [59])

conservatively biased and conservative assumptions are made regarding sequences. This includes conservative input assumptions, initial conditions, maintenance assumptions and worst coincident single failure. This analysis may be performed against acceptance criteria which may be more relaxed than that applied to AOOs (see ref. [16]), a common approach which is articulated in SSG-2 (ref. [56]). My assessment of the application of this approach is summarised in section 4.3.4, however, the general approach meets my expectations for including conservatism for deterministic analysis of design basis faults, as articulated in SAP FA.7 (ref. [28]) and SSG-2 (ref. [56]).

120. The DEC scenarios are analysed to determine the performance of safety functions within DL4 and demonstrate the effectiveness of DEC safety features. For DL4a functions, the acceptance criteria are based on avoiding core damage (see section 15.1.4 of Chapter 15.1 of the PSR, ref. [14]). The conservative assumptions related to plant availability are relaxed for DEC-A analysis (EX-DSA), however, where possible, the analysis of DEC-A events still largely adopts the methods applied in CN-DSA (e.g. conservative initial conditions). The RP's approach, therefore, may be considered more conservative than the approach to DECs without significant fuel degradation as described in SSG-2 (ref. [56]). DEC-B scenarios are analysed on a best estimate basis (EX-DSA). This is covered in further detail in section 4.3.5; however, overall, I judge that the approach to deterministic analysis of DECs meets my expectations, as informed by FA.6, FA.7, FA.15, FA.16 of the SAPs (ref. [28]) and SSG-2 (ref. [56]).

121. The RP's acceptance criteria for the DSA are presented in Chapter 15.3 of the PSR (ref. [16]). Although my assessment hasn't reviewed the fuel and core related criteria in detail, I have confirmed with the Fuel & Core Inspector that they are generally appropriate for the BWRX-300 design (ref. [67]). I have also confirmed that the criteria meet the intent for demonstrating RCPB and containment barriers remain intact in design basis events (SAP FA.7).

4.3.2.3. Linking of initiating faults, fault sequences and safety measures, and further use of DBA

122. The RP's 'Fault Evaluation' document (ref. [70]) lists all safety functions determined by the levels of analysis described above. The RP has added these functions to a 'Fault List' and linked them to the sequences which claim them. The 'Fault List' is a live document listing all sequences which the RP has provided to me for information on a secure document management system. The design requirements on the SSCs which deliver the listed functions are also listed and linked. However, the RP has not presented a fault schedule. As such, this is a shortfall against my expectations as informed by FA.8 of the SAPs (ref. [28]). However, for Step 2 GDA, I judge the RP's documents described above provide sufficient evidence of linking faults, sequences and measures to support the fundamental design. Noting the RP has committed to providing a fault schedule for future PCSR (see

FAP item 15.5-28 of ref. [73]), I do not consider this a significant shortfall for Step 2.

123. The RP's 'Fault Evaluation' document (Ref. [70]) identifies design requirements on the SSCs which support safety functions. Ref. [70] lists these requirements (see Table 4-1) along with the DL 2 to 4a safety functions they support (see Tables 6-1 to 6-4). I consider these design requirements important for securing the Defence Line independence claims of the RP's safety strategy (ref. [59]) described in previous section 4.3.1 and for meeting Target 4 (SAP NT.1).

124. In addition, I have found evidence of the RP using the fault analysis to identify and gather important design performance parameters for SSCs. These parameters are documented in ref. [74] with general examples including rod insertion times, valve closure times and flow rates. Limits and conditions of operation are also identified; an example is maximum initial ICS pool temperature. I consider the RP's use of its fault analysis to identify design requirements in ref. [70] and performance parameters in ref. [74] to meet my expectations of using DBA to establish engineering requirements on safety systems against FA.9 of the SAPs (ref. [28]). I am content the RP has committed to further use of the DBA to derive Operating Rules for the future PCSR under FAP item 15.5-37 of ref. [73].

4.3.2.4. Summary

125. In summary, the RP's approach to fault analysis allows for the identification of faults, grouping and bounding, categorisation of faults, identification of safety measures, a graded approach to conservatism in the demonstration of effectiveness, and a demonstration that appropriate acceptance criteria are met. I also judge that the RP has adequately demonstrated a linking between the fault analysis and engineering requirements. I, therefore, judge that the RP's general approach aligns with my expectations, as informed by SAPs NT.1, FA.1-9, FA.15 & FA.16 (ref. [28]), NS-TAST-GD-006, NS-TAST-GD-007 (ref. [29]), SSR2/1 (ref. [55]) and SSG-2 (ref. [56]).

4.3.3. Identification of Faults (DBAs) and Event Sequences (DEC-As)

126. My expectation is that systematic, auditable, and comprehensive fault identification should be carried out to identify the faults which could give rise to a significant radiological consequence. In particular, it is my expectation that design basis methodologies are applied to faults which have a frequency and unmitigated radiological consequence which exceed Target 4 (SAP NT.1).

127. It is also my expectation that all initiating events with a frequency greater than $1x10^{-5}$ pa (SAP FA.5), or an event sequence frequency greater than $1x10^{-7}$ pa (SAP FA.6) should be analysed using design basis analysis techniques. In addition, I expect that CCF is considered. Informed by ONR's

guidance for SAP EDR.3 (ref. [28]), typically, I expect that the likelihood of CCF claims be limited to $1x10^{-5}$ for non-complex systems. With this in mind, I expect the RP to identify sequences which consider consequential failures and common cause failures of protection measures, as appropriate. As stated in NS-TAST-GD-006 (ref. [29]), this typically manifests in the identification of diverse safety measures for frequent faults.

128. The RP claims its fault identification methods cover all sources of radioactivity. The RP's methods for identifying postulated initiating events (PIEs) fall into two types. Functional failure analysis (FFA), which is mainly reliant on failure modes and effects analysis (FMEA), is used to identify functional failures of systems covering both single random failure and common causes. This includes failures which could lead to an internal hazard leading to a PIE. Human failure event analysis (HFEA) is used to identify the errors which could be made by personnel during normal operations or planned maintenance activities. The RP also supplement these with fault lists identified from its access to extensive operating experience of BWRs.

129. The initiating events are grouped into PIEs and presented in the live 'Fault List', previously described. This lists and further groups the PIEs for fault sequence development and fault analysis. For Step 2 of GDA the RP has provided an extensive detailed list of PIEs in a 'Fault Evaluation' document (ref. [70]). The method of grouping of PIEs with similar fault progression and system response is a common approach when demonstrating the effectiveness of safety measures, and aligns with my expectations informed by SAP FA.5 (ref. [28]) and SSG-2 (ref. [56]).

130. In general, it is my expectation that multiple methods are applied, typically including HAZOP, to identify initiating events. My sample is, therefore, of importance to gain confidence in the comprehensiveness of the fault identification. To gain confidence in the application of this approach, I have sampled both LOCAs (covered in section 4.3.3.1) and overpressure faults (covered in section 4.3.3.2).

4.3.3.1. LOCAs

131. For loss of coolant accidents, the primary concern is retention of sufficient inventory to maintain the water level above the core (and to enable ICS to perform effectively), and to remove heat from the containment. When considering sequences in the following section, I have therefore focused on the potential CCF of the principal means of delivering heat removal and containment functions.

132. Large isolable loss of coolant accidents result in rapid closure of the RIVs (assumed within 10s) to avoid excessive loss of coolant inventory while also limiting the steam discharge. Depending on whether the steam discharge is within containment or not, then Hydraulic Scram (and ICS) will either initiate on high containment pressure or line break indication. Small unisolable loss

of coolant accidents result in Hydraulic Scram on low RPV pressure with ICS initiating on low RPV water level.

Identification of Initiating Events

133. The RP has identified the following pipe break scenarios as PIEs:

- Double ended guillotine pipe breaks arising outboard of the twin RIVs on all large reactor coolant lines (>19mm diameter):
    - Main Steam (MS) lines both within and beyond containment
    - Feedwater (FW) lines
    - CUW (Clean-Up Water) lines
    - ICS lines (steam supply and condensate return lines)
- Pipe breaks arising on small reactor coolant lines both within and beyond containment

134. Based on their frequency, and because they result from single failures, these initiating events have been categorised as DBAs (frequency between $1x10^{-2}$ and $1x10^{-5}$ pa). Whilst I have not assessed the hazard identification techniques in detail, the range of pipe breaks appears comprehensive with the following exceptions:

- Multiple pipe breaks which might result from secondary dynamic effects (internal hazards such as pipe whip) arising from a pipe break within a High Energy Line (HEL); and
- Breaks arising inboard of the RIVs at the connection between RIVs and the RPV.

135. The methods of assessment of the indirect consequences of a pipe-break leading to multiple pipe-breaks is not novel. I note the RP has treated this as an internal hazard (see Chapter 15.7 of ref. [20]) and has committed under FAP item 15.7-63 of ref. [73] to develop an approach based on Break Exclusion Zone (BEZ). ONR's Internal Hazards Inspector (ref. [75]) found that the RP has developed an approach which meets UK expectation concerning assessment of consequences and is content this would be applied by a future safety case under FAP item 15.7-63 (ref. [73]). On this basis and because I consider there are several options available for mitigating indirect consequences, if found to be significant, I am content this is not a fundamental shortfall that cannot be resolved in future.

136. However, I consider the RIVs to be both novel and fundamental to the BWRX-300 design. An inboard break would undermine the function of the RIVs and potentially pose challenges to inventory retention required for core coverage and ICS. In response to RQ-01870 (ref. [76]), the RP has

confirmed there are no high integrity claims placed upon the RIVs which might justify exclusion of the break. I therefore judge that the RP has not provided a justification for exclusion of this fault from its fault identification. Although the RP has not provided an initiating event frequency for such faults, I judge that they may lie in the DBA or DEC-A region and expect a demonstration of fault tolerability against such faults.

137. In response to RQ-01763 (ref. [77]), the RP has acknowledged these inboard breaks to require further deterministic safety analysis. In response to RQ-01770 (ref. [78]) the RP has described the outcome of preliminary analysis they have undertaken of these breaks. The RP has also shared the analysis reports with me for information on the secure document management system. This analysis places claims upon making-up inventory using the control rod drive hydraulic sub-system to prevent the core being damaged, which I judge has the potential to meet my expectations. While I recognise that the design intent of the BWRX-300 may have always considered these scenarios, the GDA SSSE does not set out what the safety case is for these LOCAs. It is therefore unclear what claims and arguments are being made, and what evidence or analysis is currently available and what still needs to be provided to support the claims (for example the future application of high integrity classification and BEZ processes, and showing the relevant components achieve the desired performance and reliability requirements). I have therefore raised a Regulatory Observation (RO-BWRX300-004 ref. [79]) to track resolution for future PCSR. Until then, I am content the RP has acknowledged this event and are undertaking the appropriate work to cover it. I am content that the Resolution Plan (ref. [80]) which the RP have now produced demonstrates its understanding of the gap and has identified a credible means to resolve it (supported by commitments under FAP item 15.5-404 of ref. [73]). While I consider this a shortfall against my expectations for identification of faults, as informed by SAP FA.5 (ref. [28]), based on the information provided, I do not consider this to be a fundamental shortfall that cannot be resolved in the future.

Identification of Sequences

138. In this section, I summarise my assessment of the RP's approach to consideration of CCF of the principle means of protection for appropriate faults, which the RP treats as DEC-A sequences.

139. I have found the RP's consideration of sequences cover concurrent CCF of the PPS to isolate the break. In such cases, the back-up DPS offers a further $1x10^{-3}$ reduction in sequence frequency, meeting my expectations related to diverse protection.

140. However, I consider there are two sequences that are not identified by the RP, which have the potential to have sequence frequency above the typical 'cut off' of $1x10^{-7}$ pa (SAP FA.6):

- Large outboard pipe breaks in the ICS with concurrent failure of the PPS to close the RIVs, noting there is no DPS function to isolate the ICS should the PPS fail (see Section 3.1 and the response to RQ-01761 concerning C&I, ref. [81]); and

- Large outboard pipe breaks with concurrent mechanical CCF of a pair of RIVs.

141. I judge that this to be a shortfall against my expectations, informed by SAPs FA.6 and EDR.3 (ref. [28]). Akin to inboard breaks, these sequences potentially challenge core coverage and ICS operation. The RP's response to RQ-01770 (ref. [78]), as discussed for inboard breaks, has acknowledged these sequences to require further analysis. Therefore, these sequences are also covered by RO-BWRX300-004 (ref. [79]) and associated RP's commitments, as discussed previously.

142. Whilst the above is a shortfall against my expectations for identification of sequences, as informed by SAP FA.6 (ref. [28]), the RP has claimed that it has undertaken analysis to show that sufficient protection will be provided by the making-up of inventory using the control rod drive hydraulic sub-system to prevent core damage (as stated in RQ-01770, ref. [78]). I, therefore, do not consider this to be a fundamental shortfall that cannot be resolved.

143. Regarding the lack of DPS function to close RIVs on the ICS, the isolation of ICS has competing safety demands. On the one hand, it is desirable to improve the reliability of RIV closure for an ICS break; on the other hand, introducing more isolation provision may increase the probability of inadvertent ICS isolation. Since there are trade-offs, I return to ICS breaks in ALARP section 4.3.10.

4.3.3.2. Over-Pressure Events

144. I have sampled overpressure events to target the RP's claims on shutdown provisions RPV and over-pressure protection (by heat removal) . Specifically, this relates to the Hydraulic Scram and ICS safety functions.

145. Overpressure events result in rapid closure of MS lines and rapid isolation of the main condenser from the reactor while it is operating at power. This causes a sudden increase in reactor pressure which collapses voids within the core leading to a reactivity insertion and Hydraulic Scram on high neutron flux. The RP's fault analysis assumes that this achieves safe shutdown within 5s accounting for signal delay and valid for reactor pressures up to the design limit (see Table 15.5-5 of ref. [18]). Following shutdown, the reactor pressures continue to increase until the ICS is initiated on high pressure to control the pressure and deliver DHR (Decay Heat Removal).

Identification of Initiating Events

146. I have found the RP's identification of initiating events includes the following over-pressure events:

- A loss of load on the turbine resulting in sudden closure of the Turbine Stop Valves (TSVs) (noting these close much faster than RIVs do);
- A loss of preferred power (LOPP) resulting in closure of the Turbine Control Valves (TCVs) due to the loss of power; and
- Spurious closure of any (or all) of the main steam and feedwater RIVs.

147. These events have been categorised as DBAs (frequency between $1x10^{-2}$ and $1x10^{-5}$ pa) which meets my expectation of SAP FA.5 (ref. [28]).

148. In the sections below, I summarise my assessment of the RP's approach to consideration of CCF of the principle means of protection, which the RP treats as DEC-A sequences. I cover CCF of Hydraulic Scram first, then the ICS.

Identification of Sequences Concerning CCF of Hydraulic Scram

149. I have found the RPs consideration DEC-A sequences to cover the following:

- Concurrent failure of both the PPS and the DPS to initiate Hydraulic Scram; and
- Mechanical CCF of the Hydraulic Scram.

150. Both sequences place reliance on alternative shutdown via DPS and motorised CR run-in. The RP consider these sequences to be less frequent than $1x10^{-5}$ pa and categorised as DEC-As based on the following assumptions:

- A PIE frequency of once per year is assigned to over-pressure events; and
- A $2.1x10^{-6}$ pfd (probability of failure on demand) is assigned to the Hydraulic Scram.

151. I consider the RP's assumptions of PIE frequency reasonable while I consider the pfd for joint loss of PPS and DPS to be consistent with the claimed independence of DL3 and DL4a and their integrity targets. However, I note the reliability assigned to Hydraulic Scram is very high (~10^{-6} pfd) and could challenge expectations of what is reasonably supportable.

152. In response to RQ-01875 (ref. [82]), the RP has provided further arguments to support its claim:

- Firstly, it is underpinned by assessment covering a full range of component failures and reliability data used by the US NRC to cover General Electric Reactor Protection Systems (NUREG/CR-5500 Volume III) informed by OPEX (Operating Experience) across the US BWR fleet;

- Secondly the RP claims, a high fault tolerance is provided by proven design features, such as:

    - Failsafe Scram valves on each hydraulic line which spring open on loss of air;

    - Two redundant pilot solenoid valves on each air line, which failsafe on loss of power and are each served by a different division of load drivers and manual switches; and

    - Independent Alternative Rod Insertion (ARI) valves on each air line which fail safe on loss of power.

- Thirdly, there is considerable redundancy amongst rods to allow safe shutdown. The RP has clarified that its claim is based on 19 out of 57 rods (33%) failing to insert, which is a general target based on probabilistic studies. However, the RP has provided evidence that the BWRX-300 betters this redundancy. This is deterministic analysis which demonstrates it can achieve an interim safe stable state at reduced power using the weakest 50% of its rods and the turbine bypass (see 15.5.5.22 of ref. [18]).

153. Whilst the above provides confidence in the high reliability claim, I would expect a future safety case to incorporate the evidence of response to RQ-01875 (ref. [82]) and provide further assurance. Nevertheless, I judge the arguments reasonable to justify treating sequences with CCF of the Hydraulic Scram to be DEC-A sequences.

154. The RP's submitted fault analysis has not covered further sequences involving failure of the motorised CR run-in, which lead to a joint failure to Scram. This sequence could potentially arise from mechanical CCF of the rods to insert, rendering both Hydraulic Scram and motorised run-in ineffective. I note the RP has provided an alternative diverse shutdown system (BIS) with sufficient liquid absorber to ensure safe shutdown (ref. [7]). Under FAP item 15.5-29 of ref. [73] I note the RP has committed to demonstrate the functional capability and reliability of BIS if needed.

Identification of Sequences Concerning CCF of ICS

155. The RP has not presented any DEC-A sequences in which there is a CCF of the ICS to deliver its heat removal function. The RP places high reliability claims upon the ICS (~10^{-7} pfd), making the sequence of overpressure faults with failure of ICS to initiate very low frequency. The RP, therefore, has not identified any further diverse safety measures for heat removal during

frequent faults. Whilst this initially appears to be a shortfall against my expectations for SAPs FA.6 and EDR.3 (ref. [28]), I note the following features lend credibility to a high reliability claim:

- Only one ICS train is required for the ICS to be shown effective against DBAs (see section 4.3.4);
- For an ICS train to initiate, only one of two diverse parallel valves on the condensate return line are required to open. ONR's Mechanical Engineering assessment has found that there is adequate diversity between these valves (ref. [83]);
- ICS trains automatically initiate on loss of power, noting both valves are designed to fail safe fully open using stored spring energy upon a loss of control signal, control power, or pneumatic supply with no actuation signals required from PPS or DPS;
- ICS trains are automatically initiated by PPS and DPS or manually initiated by the operator using manual switches (located in the MCR and SCR) which interrupt power to the solenoids in the fail-safe valve actuating circuits; and
- The Isolation Condenser Pools Cooling and Clean-Up System (ICC) provides control and monitoring in the ICS pools, the adequacy of which were subject to ONR's Chemistry assessment (ref. [84]). This covers water chemistry, level and temperature and includes a means of ICS leak detection, providing confidence that any degradation of ICS safety functionality or precursors leading to degradation would be detected (e.g. corrosion impairing heat exchange, heat exchanger tube failure or foreign material ingress).

156. The very low pfd assessed in the PSA (ref. [85]) does not include passive failure of natural circulation of the ICS. However, ONR's PSA assessment has found that adequate justification has been provided to exclude these contributions to the pfd (ref. [86]) during Step 2 on the basis of low sensitivity to inclusion, with further work to be completed under FAP item 15.6-48 (ref. [73]).

157. I also note that there is ongoing work regarding latent human error contributions to the pfd (committed to under FAP item 15.4-191 of ref. [73]). However, should this result in challenges to the ICS reliability, I judge that there are available means to minimise the human error contributions that would not challenge the fundamental design.

158. Furthermore, whilst I note that assessment of hazard-initiated sequences remains outstanding (committed to under FAP item 15.5-30 of ref. [73]), I have confidence that the segregated design of the ICS pools by reinforced structural walls would help maintain the high reliability claims against potential challenges.

159. Moreover, I consider the deterministic analysis of DBAs (which I discuss in detail in section 4.3.4.1) provides confidence against 'cliff edge' consequences arising from challenges to ICS performance. This shows a single ICS train capable of providing large margin to safety limits, despite containing various conservative assumptions (including a 30% assumed reduction in performance against test), indicating that degraded performance (e.g. fouling of the heat exchanger tubes) can be readily tolerated without loss of ICS safety function;

160. Based on all the above, I judge that the RP's high reliability claim on the ICS is supportable at Step 2. However, I note that I have not assessed the detailed evidence underpinning the ICS pfd. In addition, there is ongoing work regarding contributors to the pfd. A future safety case will therefore need to provide further detailed evidence to fully underpin the claim. Because of these reasons, I judge that further assessment, beyond step 2, of forthcoming evidence will be required.

161. Notwithstanding further work required to justify the high reliability claim of the ICS, I note that the BWRX-300 includes design provisions that, whilst not credited in the deterministic safety case, mitigate my concerns regarding CCF of the ICS. In particular, I note the design includes features (comprising make-up from the control rod drive hydraulic sub-system, the UPR and the containment vent) which potentially offers a viable diverse means of heat removal and has the potential to contribute to demonstrating risks reduced ALARP. The RP has committed to considering further fault sequences as part of FAP item 15.5-30 (ref. [73]), and I expect that fault sequences including CCF of the ICS are analysed in the future.

162. In summary, whilst the RP's reliability claims on the ICS are greater than I would typically expect, I judge that it is plausible that the reliability claims can be justified with further evidence. Moreover, whilst no deterministic claims are placed on alternative means of heat removal, the BWRX-300 does include design provisions which could potentially be claimed in a future ALARP justification.

4.3.3.3. Summary of Identification of Faults and Event Sequences

163. I have found potential shortfalls in the RP's safety case against my expectations related to the identification of the following events and sequences:

- Large un-isolable or non-isolated LOCAs :
    - Identification of breaks between the RPV and the RIVs
    - Mechanical CCF of a pair of RIVs following a break
    - Failure of the PPS to initiate RIV closure following the break of ICS pipework

- CCF of the rods to insert during faults; and
- CCF of the ICS to initiate during faults.

164. However, I do not consider that these present a fundamental shortfall with the design for the following reasons:

- Large un-isolable or non-isolated LOCAs:
    - In response to RQ-01763 (ref. [77]) and RQ-01770 (ref. [78]) the RP has given me confidence it is undertaking the necessary analysis to demonstrate that acceptance criteria are met covering the range of large non-isolable and non-isolated LOCA sequences. This analysis features claims on the control rod drive hydraulic sub-system to deliver make-up to keep the core adequately cooled and avoid 'cliff-edge' consequences;
    - In response to RQ-01870 (ref. [76]) raised by the Structural Integrity inspector, the RP has given me confidence it will assign a suitable safety classification to the RIV/RPV connection to appropriately limit the likelihood of large non-isolable LOCAs and their consequences;
    - In response to RO-BWRX300-004 (ref. [79]), the RP have produced a Resolution Plan (ref. [80]) which jointly covers the above matters (with further reasoning for ICS LOCAs given in ALARP section 4.3.10.2);
- Under FAP item 15.5-29 of ref. [73] the RP has recognised ONR expectations related to CCF of the rods to insert and has committed to demonstrate the functional capability and reliability of BIS if needed (with further reasoning given in ALARP section 4.3.10.3); and
- While the RP's reliability claims on the ICS are very high, I consider the various aspects of its design and safety assessment lend credibility to these claims and give me confidence there is no fundamental shortfall for Step 2. However, I expect these claims to be further justified within a future safety case, where I would also expect further consideration of sequences involving CCF of the ICS with a view to strengthening defence-in-depth and demonstrating risks reduced ALARP (under FAP item 15.5-30 of ref. [73] described further below).

165. Overall, whilst I have found gaps in the RP's approach to identification of the individual faults and sequences above, I am confident the RP can address these shortfalls in a future BWRX-300 safety case without challenging the fundamental design. Despite the limited hazard identification methods employed, I am content with the adequacy of the RP's fault identification approach and with the RP's overall commitment to apply it to other faults under FAP item 15.5-30 (ref. [73]). This FAP is specified to cover faults in all

reactor operational modes, non-reactor faults, faults arising in support systems, faults arising from hazards and faults where there are further failures of safety measures. In particular, I take confidence from the RP's fault evaluation document (ref. [70]) which already identifies and categorises the faults relating to start-up and shutdown operations.

166. On this basis I judge the RP's approach can achieve adequacy and fully meet my expectations informed by SAPs FA.5, FA.6 (ref. [28]) and SSG-2 (ref. [56]).

4.3.4. Effectiveness of Safety Measures for DBAs and DEC-A sequences

167. It is my expectation that deterministic safety analysis should be performed to demonstrate the effectiveness of identified safety measures in order to reduce risks ALARP. In doing so, I expect that appropriate conservatism is employed, and that it is demonstrated that for design basis faults and sequences the safety criteria for fuel and containment are met, and radiological consequences are within Target 4 (SAP NT.1). My expectations are informed by FA.6, FA.7 and NT.1 of ONR SAPs (ref. [28]) and SSG-2 (ref. [56]).

168. When demonstrating the effectiveness of safety measures for DBAs, aligned with my expectations as informed by SAP FA.6 (ref. [28]), I expect the following assumptions are made:

- Sequences account for consequential failure, single failure and maintenance unavailability; and
- The worst possible initial conditions and plant states.

169. In addition, for DBAs I expect that the analysis is performed in a conservative manner and does not take credit for the correct performance of safety related systems (such as the APS). I also expect that it is demonstrated that no barrier to release are compromised, and if they are that the last remaining barrier to release is not challenged. For the latter, I expect that suitable acceptance criteria are applied and that the deterministic analysis demonstrates that these are met. These expectations are guided by SAP FA.7 (ref. [28]).

170. For DEC-A, aligned with NS-TAST-GD-006 (ref. [29]), FA.7 (ref. [28]) and SSG-2 [56], I consider conservatism in the analysis can be reduced. For example, I do not expect that an additional single failure of safety systems is considered.

171. As stated previously, I have chosen to sample LOCAs and Overpressure faults for the following reasons:

- LOCAs – LOCAs are challenging for RIV closure times to retain sufficient water inventory to enable ICS and maintain core coverage and are challenging for containment overpressure and overtemperature. LOCAs are also challenging for demonstrating an adequate mission time for the ICS, since fewer trains are credited due to the loss of one train of ICS due to the break; and

- RPV Overpressure – Overpressure results in a fast reactivity insertion and overpressure of the RPV. This places significant demand on the Hydraulic Scram and ICS to overturn reactivity insertion and reduce pressures, respectively.

172. The following sub-sections summarise my assessment against the above expectations of how the RP has performed that analysis on design basis fault sequences and demonstrated safety measures effective based on my sampling of evidence.

4.3.4.1. Effectiveness of Safety Measures against LOCAs

173. In general, the main objective of the RP's CN-DSA approach is to demonstrate the effectiveness of the principal DL3 functions and is applied to DBAs only. However, for LOCAs, the RP has gone beyond this and have aimed to apply CN-DSA to DEC-As. In result, the RP has aimed to demonstrate both DL3 and 'back-up' diverse DL4a functions in a conservative manner.

174. The large LOCA sequences covered by the RP's analysis are described in section 4.3.3.1 and require the following key safety measures to deploy: Hydraulic Scram, RIVs, PCS and ICS. These may be initiated on different parameters depending on whether the pipe-break takes place outside containment or inside. Overpressure and over-temperature protection of the containment due to mass and energy releases into containment is provided by the PCCS, which does not require initiation but is continuously available to safeguard the structures from the effects.

175. Deterministic analysis of DBA and DEC-A LOCA faults has been performed using the TRACG and GOTHIC codes. My assessment of these codes is summarised in Section 4.3.8.

176. The safety criteria for LOCAs are presented in Table 15.3-2 of ref. [16]. For the fuel and core, the RP presents safety criteria such as PCT (Peak Clad Temperature) and maximum allowable corrosion. The Fuel and Core Inspector has found these to be consistent with the criteria which applied to GE14 fuel previously covered by GDA for ABWR (ref. [67]). So together, we judge these are well founded criteria for BWRs and appropriate for the use in BWRX-300.

177. For success criteria of the PCCS in adequately preventing overpressure and over-temperature of the SCCV, the RP present the limits 515kPa and

165.6°C. The Civil Engineering inspector has reviewed the RP's approach to deriving performance limits based on its engineering analysis of the leak-tight performance of containment under hot pressurised conditions and accounting for seismic, all of which he has considered to be appropriate (ref. [87]).

RIVs and ICS

178. An important aspect of LOCAs is the requirement to retain sufficient coolant to enable ICS and maintaining a water level to cover the core, and to provide long term heat removal. The deterministic analysis therefore sets out to demonstrate that the plant response (including trip settings and RIV closure times), adequately achieves these objectives. In performing this analysis, the following assumptions have been made by the RP:

- concurrent single failure within PPS (or the DPS)
- consequential failure of a train of ICS to deploy due to the break[10]
- concurrent single failure of a condensate return line valve within any remaining successful ICS
- concurrent failure of a single RIV within a twinned RIV pair to close
- no credit has been taken for containment back-pressure in suppressing further loss of coolant once discharge rates fall to sub-sonic levels

179. The RP claim that no maintenance of the ICS system will be performed during power operations. I consider this availability assumption will need securing with Operating Rules for future PCSR (under FAP item 15.5-37 of ref. [73]).

180. The above assumptions essentially result in only one out of three trains of ICS being claimed. In addition, the RP has applied conservative assumptions to the initial conditions and plant performance. For example, in response to RQ-01768 (ref. [88]) the RP has provided evidence of a 30% assumed reduction in heat transfer below validated values, penalising performance further and giving confidence against uncertainties.

181. For large LOCAs, the analysis demonstrates that PCT and oxidation limits are comfortably met. The analysis demonstrates that a RIV closure time of 10 seconds is sufficient in retaining sufficient inventory to keep the core covered and therefore maintaining PCT limits in the longer term. The analysis also demonstrates that the ICS is effective in removing decay heat and reducing RPV pressures and temperatures following the initial transient.

[10] If the LOCA arises on an ICS train, then the PPS will isolate it at the RIVs in response to line-break detection.

182. Due to their location, some small LOCAs are not isolable by the RIVs. Unlike large LOCAs, small un-isolable LOCAs therefore have the potential to lead to coolant levels falling below top of core in the long term. In response to RQ-01768 (ref. [88]) the RP has provided further evidence that the core remains adequately cooled and PCT limits are satisfied.

183. For all LOCAs I have found the analysis demonstrates the response to be effective in enabling the ICS to keep the core covered and protect fuel safety limits. Clad temperatures are shown to remain below normal operating levels (see 15.5.4.5 of ref. [18]).

184. Concerning adequacy of ICS mission time, the RP claims one ICS train can provide adequate DHR (Decay Heat Removal) over 72hrs. In response to RQ-01768 (ref. [88]) the RP has provided a comprehensive list of penalising assumptions when analysing the mission time of ICS. For example, the RP assumes conservative decay heat curves and unrealistic ICS initial pool temperatures. I consider this gives adequate assurance of margin against 'cliff edge' loss after 72hrs.

185. In conclusion, I judge that the RP's analysis of the effectiveness of the RIVs and ICS incorporates adequate conservatism and demonstrates that relevant safety criteria are met. In my judgement, the RP has provided confidence that there is sufficient redundancy in the RIVs and ICS to maintain relevant acceptance criteria during LOCA events. Therefore, I consider that my expectations, as informed by SAP FA.6 and FA.7 (ref. [28]) and SSG-2 (ref. [56]), are met.

PCCS

186. For large LOCAs causing steam discharge into containment, the primary concern is removing sufficient heat via the PCCS to reduce temperature and pressure in the containment that could challenge its structural integrity.

187. In analysing the effectiveness of the PCCS, the RP has made the following assumptions, which it claims penalise the transient:

- Concurrent failure of the outboard CIV to close which does not worsen coolant inventory but worsens the steam discharge into containment [11];
- Concurrent LOPP[12];

[11] Relevant to all large pipes except for the ICS trains which only extend as far as the ICS pools in a closed loop and do not have outboard CIVs.

[12] This worsens the sequence since it means no credit is taken for the Containment Cooling System (CCS), a Safety Class 3 'make-ready' system which provides normal cooling to the containment.

- Initial conditions appropriately biased to give conservative discharge rates into containment;
- No credit taken for conduction from the steel shell into the concrete; and
- Allows loss of one out of three trains of PCCS (confirmed in Mechanical Engineering Inspector's report, ref. [83] which reports 50% performance achievable with one train).

188. The worst LOCA for containment is the MS line pipe break where containment pressures and temperatures reach 423kPa and 134^{o}C compared to acceptance limits of 515kPa and 165.6^{o}C respectively (ref. [18]).

189. For the large LOCAs causing steam discharge into containment, I have found the analysis demonstrates the PCCS to be effective in protecting the structural limits of the containment. I consider that my findings from the RP's submission (ref. [18]), further corroborated by my engagements (ref. [89]), are consistent with the observations of the overseas regulators (see Appendix 3 – Findings by other regulators).

190. In conclusion, for DBAs identified by the RP, I consider the analyses demonstrates that the PCCS is effective in maintaining pressures and temperatures within acceptance criteria. The RP has applied suitable conservatism in input assumptions and availability assumption. This, therefore, meets my expectations as informed by SAPs FA.6 and FA.7 (ref. [28]) and SSG-2 (ref. [56]) for Step 2 GDA.

4.3.4.2. Effectiveness of Safety Measures against Overpressure Events

191. The over-pressure event sequences covered by the RP's analysis are described in section 4.3.3.2. Aligned with its approach to deterministic analysis, the RP has applied CN-DSA to DBAs, and EX-DSA to DEC-A sequences.

192. The RP has performed deterministic analysis using the TRAC-G code. A summary of my assessment of TRACG can be found in Section 4.3.8.

193. Over-pressure safety limits for the Reactor Coolant Pressure Boundary (RCPB) are presented in Table 15.3-2 of ref. [16]. The Mechanical Engineering inspector has reviewed the RP's approach to over-pressure protection and limits as appropriate (ref. [83]).

194. Fuel safety criteria concerning the fuel are the same as for LOCAs, and Hydraulic Scram and ICS are similarly required to deploy. However, unlike LOCAs, the rapid rise in reactivity due to the collapse of voids prior to the Scram, increases clad temperatures beyond normal operating levels and reduces margins to boiling transition. The Fuel and Core inspector is content with the margins to boiling transition (ref. [67]). So together, we judge that the acceptance criteria applied to overpressure transients is appropriate.

195. For the DBA sequences, the CN-DSA has applied the following conservative biases and assumptions:

- APS, a class 3 safety related system, fails to take pre-emptive action to scram the reactor which would otherwise reduce the severity of the over-pressure transient[13];
- Pressure control functions fail to open the turbine bypass lines and dump excess steam to the main condenser;
- Level control functions fail to trip the FW pumps, which leads to increased RPV pressure;
- Concurrent single failure within PPS (and/or the DPS);
- Concurrent failure of the 'first-up' ICS train to deploy[14];
- Concurrent single failure of a condensate return line valve within the successful ICS to open; and
- All relevant thermal hydraulic parameters are conservatively biased by at least one standard deviation.

196. I judge that the above assumptions lead to a conservative outcome in the demonstration of the effectiveness of both the Hydraulic Scram and ICS. Based on this, I am content that the RP's approach adopts sufficient conservatism in its deterministic analysis, meeting my expectations as informed by SAPs FA.6 and FA.7 (ref. [28]) and SSG-2 (ref [56]).

197. I have found the analysis of the worst-case DBA sequence presented in Chapter 15.5 (ref. [18]) gives predictions of high margin to key safety limits despite the conservative biasing:

- peak clad temperature of 511.8^{o}C compared to 1204^{o}C acceptance limit
- peak reactor pressure of 8.69MPa compared to 12.41MPa acceptance limit

198. For all over-pressure DBAs identified by the RP, the analysis, therefore, demonstrates that the Hydraulic Scram and ICS are sufficient to prevent the RP's safety limits from being exceeded, with considerable margin. The RP's analysis also provides confidence that there is sufficient redundancy within the Hydraulic Scram and ICS to remain effective during overpressure DBAs when conservative availability assumptions are applied. I consider the

[13] APS is prompted by parameters relating to services essential for reactor operation while PPS or DPS are prompted by parameters relating directly to reactor safety

[14] ICS trains have staggered initiation set-points for high RPV pressure

analyses meet my fundamental expectations of FA.6 and FA.7 (ref. [28]) for Step 2 of GDA and adequately demonstrate the effectiveness of the claimed safety measures.

199. For the DEC sequences involving CCF of the Hydraulic Scram, the RP places claims on the motorised CR run-in. The EX-DSA credits all 3 trains of ICS to prevent over-pressure limits being exceeded whilst the rods are driven in at a slower speed than Hydraulic Scram. The DEC-A analysis demonstrates that for sequences in which Hydraulic Scram has failed, the CR motorised run in effectively limits PCT and RPV pressure. The RP's approach for relaxing conservative assumptions for low frequency sequences is aligned with my expectations, as informed by NS-TAST-GD-006 (ref. [29]) and SSG-2 (ref. [56]). I am, therefore, content that the RP's analysis demonstrates the effectiveness of motorised CR run-in and ICS for the identified DEC-A sequences.

200. In summary, the RP's analysis demonstrates the effectiveness of ICS and Hydraulic Scram for identified DBAs, and the motorised run-in and ICS for identified DEC-As. I judge that the RP's approach to analysis of over-pressure transients meets my expectations, as informed by FA.6, FA.7 (ref. [28]), NS-TAST-GD-006 (ref. [29]) and SSG-2 (ref. [56]).

4.3.4.3. Summary of Effectiveness of Safety Measures

201. I judge that the RP's analysis includes appropriate assumptions regarding the availability of safety systems, and takes appropriate account of the worst single failure, consequential failures, maintenance assumptions and the incorrect operation of safety related equipment.

202. The RP's approach also incorporates conservatism, uses appropriate safety limits to demonstrate that fuel, RPV and containment remains intact, as appropriate, and demonstrates sufficient safety margin.

203. In my judgement, the RP has provided sufficient demonstration of the effectiveness of Hydraulic Scram, motorised CR run-in, RIVs, ICS and PCCS for the appropriate DBAs and DEC-A sequences.

204. By meeting my expectations for deterministic analysis of design basis fault sequences, the BWRX-300 design demonstrates the passive safety systems of both ICS and PCS to be sufficiently redundant and effective for providing adequate core cooling, over-pressure protection and containment.

205. This, therefore, meets my expectations, as informed by FA.6, FA.7 (ref. [28]), NS-TAST-GD-006 (ref. [29]) and SSG-2 (ref. [56]).

4.3.5. Severe Accident Analysis (DEC-B)

4.3.5.1. Severe Accident Analysis Approach

206. My expectations of the Severe Accident Analysis (SAA) are listed below:

- Sequences which have the potential to lead to a severe accident should be identified (SAP FA.15);
- Severe accident progression and phenomena should be demonstrated to be understood (SAP FA.15);
- Analysis should be used in the consideration of further risk-reducing features and that they are demonstrated to be effective (SAP FA.16);
- Analysis should be performed in a manner complementary to the PSA (SAP FA.25); and
- This should form part of a demonstration that sequences that have the potential to lead to large or early radioactive releases are practically eliminated[15].

207. In addition to the SAPs identified above, my expectations are informed by SSG-2 (ref. [56]), SSG-88 (ref. [57]), SAP FA.15 (ref. [28]) and NS-TAST-GD-007 (ref. [29]).

208. The RP has outlined its approach to SAA in Section 15.5.6 of Chapter 15.5 of the PSR, ref. [18]. The approach can be summarised as follows:

- Selection of severe accident states based on a combination of historical experience and systematic development of PSA sequences;
- Performance of analysis of severe accident states based on a comprehensive understanding of severe accident phenomena and progression;
- Use of deterministic analysis to inform design, and to support the demonstration of the practical elimination of early or large radioactive releases from scenarios which could bypass defence in depth provisions; and
- The aim is to demonstrate that all SA phenomena which may result in containment failure are practically eliminated, whether by direct containment heating, steam explosions, MCCI (Molten Core Concrete Interaction) or combustible gas explosion.

209. The RP's SAA is provided in the following documents (noting these documents were submitted during Step 2 of the GDA as supplementary information):

[15] Practical elimination (PE) is an IAEA term and refers to the design ensuring sequences which could lead to an early or large radioactive release which might overwhelm protective actions off-site are either physically impossible or are extremely unlikely to arise with a high degree of confidence - see paragraph 4.5 of SSG-88 (ref. [57])

- Enclosure 1 BWRX-300 UK GDA DBR-0078529, Revision A, BWRX-300 Full Power Internal Event Severe Accident Analysis (ref. [90]);
- Enclosure 2 BWRX-300 007N3122, Revision 2, Darlington New Nuclear Project Severe Accident Analysis Methodology (ref. [91]); and
- Enclosure 3 BWRX UK GDA 007N6885, Revision B, BWRX-300 Darlington New Nuclear Project Severe Accident Analysis-SA Selection (ref. [92]).

210. The RP has based these submissions to UK GDA upon submissions to the Canadian Nuclear Safety Commission (CNSC), which follows the standards listed below.

- REGDOC-2.4.1 Deterministic Safety Analysis (ref. [93])
- REGDOC-2.5.2 Design of Reactor Facilities (ref. [94])[16]

211. Whilst I have not reviewed these standards in detail, they appear to align with my expectations as informed by SAPs FA.15, FA.16 (ref. [28]) and SSG-2 (ref. [56]).

212. The RP assumes that during severe accidents, so long as the containment remains intact, large or early radioactive releases are practically eliminated. The SAA, therefore, identifies sequences that lead to SA phenomena that could challenge the containment and aims to demonstrate that these phenomena can be prevented or mitigated by design. This is a common assertion made by reactor vendors. My assessment, therefore, has focused on the effectiveness of safety features to prevent containment failure, rather than whether associated numerical targets are met. An assessment of the radiological consequences will be required, particularly since one of the safety features is to vent to atmosphere via a filtered route. This is work committed to under FAP item 15.6-42 (ref. [73]) concerning the need for level 3 PSA for a future safety case. Meanwhile, I note that venting is not novel to BWRs since the containment free volume is significantly smaller than PWRs.

213. The following phenomena are identified that require severe accident mitigation:

- Steam explosions;

[16] In particular, Section 7.3.4 of Ref. [94] covers Practical Elimination where section 7.3.4.1 is relevant in setting requirements on the containment to maintain a role as a leak-tight barrier for a period which allows sufficient time for the implementation of off-site emergency procedures following the onset of core damage.

- High pressure melt ejection (HPME) and Direct Containment Heating (DCH);
- Containment bypass;
- Molten core concrete interaction (MCCI);
- Containment challenges due to overpressure or overheating; and
- High energy hydrogen combustion.

214. These are typical phenomena for severe accidents in light water reactors. IAEA's SSG-2 (ref. [56]) and SSG-88 (ref. [57]) set the expectation that sequences leading to certain phenomena should be demonstrated to be practically eliminated. This list aligns well with those related to design extension conditions of the reactor.

215. The deterministic analysis of severe accident sequences has been undertaken using MAAP (ref. [95]). Section 5.5 of Severe Accident Analysis (ref. [90]) describes how MAAP is used to model the BWRX-300 structures, containment barriers and safety features with the aim of ensuring that safety features either prevent phenomena from occurring (most phenomena) or are controlled (containment challenges due to over-pressure).

4.3.5.2. Severe Accident Sequence Selection

216. At this point in the design maturity, the RP has focused on selecting severe accident sequences for analysis to inform the design of BWRX-300 safety features against the need to prevent containment failure. Section 6.0 of Severe Accident Analysis (ref. [90]) reports these sequences to have been identified from the level 1 PSA with the following core damage scenarios prioritized for analysis due to their comparatively higher contribution to Core Damage Frequency (CDF):

- TGEN – an intact circuit, with successful scram but with a complete loss of PCS and ICS;
- MLOCA - an unisolated medium break LOCA with core exposure; and
- LLOCA - an unisolated large break LOCA with core exposure.

217. At this stage in GDA, I consider the RP's use of the Level 1 PSA to identify these severe accident scenarios for analysis to be sufficient. However, for a future safety case, I expect that both deterministic and probabilistic methods are used to derive sequences to set the design basis for DEC-B safety measures, as aligned with SSG-2 (ref. [56]). I would expect the work committed to under FAP item 15.5-30 of ref. [73] concerning completeness of fault list to cover this for future safety case.

218. For Step 2 of GDA, I consider the sequences appropriate for demonstrating effectiveness of the chosen safety features. For example, since the UPR would not be required for the large LOCA case, the TGEN case can be used to demonstrate the effectiveness of UPR. Moreover, the speed of core degradation has an impact on the amount of decay heat removal required by severe accident safety features, and the amount of hydrogen released. The chosen sequences present a range of speed of fault progression and can inform the design of various safety features. In my opinion, the sequences identified enable the demonstration of the various severe accident safety features. For Step 2 of GDA, I am therefore satisfied that the chosen sequences adequately align with my expectations for identification of severe accident scenarios, which are based on SSG-2 (ref. [56]) and FA.15 (ref. [28]). However, in future, I would expect a safety case to present further assessment of reasonably bounding cases for the demonstration of effectiveness of severe accident safety features as further work is done to complete the fault list and develop the PSA (under FAP items 15.5-30 and 15.6-42 of ref. [73]).

4.3.5.3. Severe Accident Safety Features

219. The RP has identified severe accident safety features to mitigate or prevent phenomena as described above. These safety features were in concept design and have been developed during the GDA. In response to RQ-01769 (ref. [96]), the RP has provided evidence to demonstrate that the design of severe accident features has been refined since the March 2024 design reference and is informed by findings of the severe accident analysis to cover the relevant severe accident phenomena.

Table 2 : Severe Accident Safety Features

Safety Feature	Purpose	Refinements
UPR	Prevents HPME by reducing RPV pressure via the ICS using rupture disc	Modified by adding an upstream PORV (Pilot Operated Relief Valve) which enables the UPR to be closed following its use
Corium Shield	Prevents MCCI arising after the core has melted, slumped and breached the RPV lower head to enter containment	Addition of a pedestal water addition system (PWAS). This prevents direct radiative heating of the RPV support pedestal by quenching the melt after it has breached the RPV lower head
Containment Venting	Relieves containment pressure	Addition of discharge route to an additional dedicated pool in the Reactor Building (RB).

Safety Feature	Purpose	Refinements
		This has a hardened vent stack for discharging the release out of the building following scrubbing in the pool.

220. These refinements are summarised in Table 2 above. For example, the corium shield is complemented by a pedestal water addition system (PWAS) which takes water from the IC outer pool to quench the melt. This is initiated by the melting of a fusible plug at a temperature which has been determined from the severe accident analysis to ensure the water is only added after the melt has relocated onto the shield so that a steam explosion is avoided. Based on the severe accident analysis, a material has now been selected for the shield which prevents MCCI and additional hydrogen generation. In addition, a dedicated pool and hardened vent stack is now provided to control the hydrogen and fission products the severe accident analysis predicts to be discharged through the containment vent. I am therefore satisfied that the severe accident analysis has been used to inform the design of the safety features.

221. The RP's response to RQ-01769 (ref. [96]) has also provided assurance that the fundamental aspects of the design remain unaffected by the refinements and they have no significant impact on the rest of the DSA supporting Step 2 GDA.

4.3.5.4. Effectiveness of Severe Accident Safety Features

222. The RP has presented a demonstration of the effectiveness of concept severe accident features in Severe Accident Analysis (ref. [90]). As stated in Section 4.2, I have not performed detailed assessment of the deterministic analysis of the effectiveness of severe accident safety features. However, I have reviewed ref. [90] to gain confidence in the RP's analysis and that the safety features would be effective in meeting its needs.

223. Ref. [90] presents deterministic analysis for the TGEN, MLOCA and LLOCA cases. In each case, the progression of the severe accident sequence is described, and the timing of key events is presented. For each sequence, the analysis is performed on a best estimate basis, where appropriate, which meets my expectations as informed by SAP FA.16 (ref. [28]), NS-TAST-GD-007 (ref. [29]) and SSG-2 (ref. [56]). I note that no credit has been taken for DL3 provisions in these sequences, such as PCCS, demonstrating the independence of severe accident safety features within DL4b.

224. For each phenomenon listed above, the RP present what appear to be reasonable acceptance criteria for demonstrating that the containment will remain intact. For each sequence, the RP concludes that the identified

safety features are effective in preventing severe accident phenomena that would challenge containment. The RP concludes that:

- Timing and discharge through the UPR can be sufficient to keep the RPV pressure within acceptable limits (same as for DBAs) during a severe over-pressure and prevent the RPV failure occurring at high-pressure (which could lead to HMPE and DCH);
- Containment overpressure due to steam discharge from the RPV prior to core melt, hydrogen generation in core degradation, and further gaseous and steam generation following core melt and relocation can be mitigated by the containment vent. The containment vent, and timing of venting, is sufficient to keep the containment pressure below the ultimate failure limit (taken to be 3.5 x design pressure);
- Thickness and composition of corium shield can be sufficient to prevent MCCI arising after the core has slumped further and breached the RPV lower head; and
- Timing and delivery rate of additional water can be sufficient to quench the relocated melt and keep the structures within high temperature failure limits, while avoiding a steam explosion.

225. Therefore, whilst I have not assessed the deterministic analysis in detail, I have gained confidence in the RP's approach and am satisfied that relevant safety features have been identified and appear to be effective in preventing or mitigating the relevant severe accident phenomena. At this stage, I judge that the RP's approach is aligned with my expectations, as informed by FA.15 and FA.16 of SAPs (ref. [28]), NS-TAST-GD-007 (ref. [29]) and SSG-2 (ref. [56]). For Step 2, I therefore judge that there are no fundamental shortfalls in the BWRX-300 design for mitigation of severe accident phenomena.

4.3.5.5. Severe Accident Analysis Summary

226. The RP has adequately identified phenomena that could challenge the containment and lead to a large or early release and should be prevented or mitigated.

227. The RP has identified an adequate set of severe accident sequences for development of severe accident safety features.

228. The RP has performed best estimate deterministic analysis which provides confidence that these safety features will be effective in preventing the relevant severe accident phenomena.

229. Overall, based on the above, I judge that the RP's approach to severe accident mitigation is aligned with my expectations, as informed by FA.15

and FA.16 of SAPs (ref. [28]), NS-TAST-GD-007 (ref. [29]) and SSG-2 (ref. [56]).

230. In addition, I consider the BWRX-300 severe accident safety features assigned to DL4b to be suitably complementary to the other DL provisions established by the DSA. In particular, I consider the RP to have significantly strengthened the independence of DL4b from other DLs by not taking credit for the DL3 safety measures (particularly the PCCS) in its severe accident analysis. I consider the layering of all DL provisions up to DL4b to be aligned to the defence-in-depth hierarchy described in EKP.3 of SAPs (ref. [28]) and IAEA Safety Standards SSR2/1 (ref. [55]), and I consider that the RP's DSA coupled to the severe accident analysis provides assurance of adequate independence and fault tolerance amongst the layers.

4.3.6. Approach to fault analysis of non-reactor faults, start-up and shutdown faults

231. Whilst start-up, shutdown and non-reactor faults fall outside the scope of the RP's fault analysis (Ref. [49]) they remain within scope of Step 2 of GDA. To provide assurance in general approach to deterministic analysis of non-reactor, start-up and shutdown faults, the RP has provided limited preliminary analysis.

232. At this stage, I cannot fully apply my expectations for FA.1 – FA.9 to these faults. However, I can take a view on the general approach to analysis of these faults.

233. In addition to the preliminary analysis, the RP has committed to analyse these faults for future PCSR (see FAP item 15.5-30 of ref. [73]), including:

- faults during start-up, shutdown and refuelling
- non-reactor faults associated with fuel route, spent fuel pool and wastes
- faults within support systems essential to operation
- faults arising from internal and external hazards

234. For non-reactor faults, the RP plans to adopt UK radiological criteria and produce a specification for a UK safety case manual (ref. [97]). To demonstrate this approach, the RP has presented a case for dropped fuel assembly on the core during refuelling.

235. For faults involving loss of shutdown cooling to the reactor, the RP plans to claim passive means of evaporative cooling / boil-off to demonstrate that acceptance criteria are met. The RP has presented arguments related to a limiting case (as stated in RQ-01776 response, ref. [98]).

236. In the below sub-sections, I summarise my assessment of the two proposed approaches.

4.3.6.1. Fuel Handling Accident (FHA)

237. During refuelling, the cavity above the containment is filled with water and fuel is transferred from the RPV to fuel storage racks that are at a higher elevation than the containment. In my opinion, the BWRX-300 fuel handling activities are generally comparable to (or bounded by) ABWR[17].

238. However, I consider the comparatively tall and narrow RPV could be a novel challenge to spent fuel handling over the core. I have therefore targeted my assessment of faults that could lead to dropped fuel on the core.

239. The RP has provided a consequence analysis of a drop of an irradiated fuel assembly onto the top of the core resulting in fuel damage and radioactive release - see section 15.5.8 of Ref. [18].

240. This consequence assessment has been performed against US NRC guidance relating to FHA methodology (Ref. [99]) and covers a release of iodine gas into the Reactor Building leading to an inhalation dose to reactor operators in the Control Building over the following 30 days. This is based on the following conservative assumptions:

- lifts take place 24hrs after shutdown
- all kinetic energy on impact is absorbed by the impacted fuel assemblies
- maximum reactor power history is assumed
- Caesium and other products are retained within the pool above the core
- no credit is taken for switching to emergency filtration in the Control Building

241. The RP calculate an unmitigated operator dose of 1.7mSv. This is below the BSL for Target 4 (SAP NT.1), and thus I would not expect DBA to be performed on this fault subject to confirming appropriateness of the use of the US FHA methodology to UK.

242. In my opinion, the preliminary analysis provides confidence in the RP's ability to perform consequence analysis of non-reactor faults, and that fuel handling faults are of relatively low significance. Engagement with the RP (ref. [100]) has given me confidence that the non-reactor activities are comparable to those assessed for previous BWR with good engineering practice adopted. On this basis, I have confidence that a future safety case

[17] For example, the below ground construction of BWRX-300 compared to ABWR leaves the RB floor at ground height limiting the height of cask lifts into or out of the building.

can adequately assess non-reactor faults for consideration of design basis analysis.

4.3.6.2. Loss of Shutdown Cooling

243. Whilst DBA has not been performed on shutdown and start-up faults, the RP's fault evaluation (ref. [70]) already identifies and categorises the events relating to start-up and shutdown operations.

244. In shutdown modes, heat is normally removed via a 2-train redundant active shutdown cooling system. Akin to power operations, the ICS and PCS are claimed whilst the reactor remains in a hot shutdown state and the containment and RPV are sealed. The RP claims that loss of the shutdown cooling system whilst the reactor is sealed is bounded by power operations. In my opinion, this is a reasonable assertion, since the heat load and energy stored in the reactor will be significantly lower during shutdown.

245. However, my assessment has found that during cold shutdown there are periods after the RPV head has been de-tensioned in which the ICS cannot be claimed. A loss of power, therefore, could leave the reactor in a state without any safety systems available to remove heat. This is of particular importance in states where there is no water above the RPV in order to de-tension the studs. For these periods, the RP makes the following arguments (see response to RQ-01776, ref. [98]):

- If the shutdown cooling system is lost in the short period between de-tensioning of the RPV head and refilling of the reactor cavity (see Figure 4), the water level in the RPV is sufficient to provide at least 24hrs worth of passive cooling by 'boil off'. I judge this would likely give sufficient time to take recovery action (falling back on either re-tensioning the RPV head or proceeding to re-fill the cavity) subject to having response arrangements and recovery plans in place for relevant events (e.g. loss of power supplies); and

- After the RPV head has been removed and reactor cavity refilled then the duties of the shutdown cooling system are passed to an active fuel pool cooling system. If this is lost, then the reactor cavity and equipment pools provide adequate cooling with make-up.

246. In my opinion, the RP's claims regarding adequate grace time are similar to those provided by previous requesting parties. Whilst this will require further assessment of whether the analysis is suitably conservative under the work committed to under FAP item 15.5-30 (ref. [73]), the RP's arguments provide confidence that a suitable future safety case can be made.

4.3.6.3. Summary

247. The RP's analysis of fuel handling faults has provided confidence in the general approach to consequence analysis.

248. The RP's analysis of shutdown and start-up faults has provided me with confidence in its approach to bounding arguments, and analysis of worst-case initial conditions. It has also provided me with confidence that evaporative cooling / boil-off can be claimed in a future safety case.

249. I am therefore content that the RP's approach is aligned with my general expectations, as informed by SAPs FA.1 – FA.9.

250. This, coupled with FAP item 15.5-30 (ref. [73]), provides me with confidence that a future safety case could be made.

4.3.7. Radiological Consequences

251. My assessment only covers radiological consequence assessment for DBAs and DEC-A. Assessment against Targets 7, 8 and 9 of SAP NT.1 (ref. [28]), which are used to assess against all faults, including severe accident sequences, is covered by the PSA assessment.

252. The RP has not provided radiological consequence assessment of its DBA or DEC sequences. I was, therefore, unable to carry out a detailed assessment against Target 4 of SAP NT.1 (ref. [28]). This is not unusual and was also true of previous RR SMR Step 2 GDA (ref. [71]). As in that case, the RP has applied safety criteria that avoids fuel failure and has demonstrated that for the DBAs and DEC-A sequences identified, those criteria are met. I have, therefore, gained confidence that future radiological consequence assessment will not challenge my expectations for Target 4 of SAP NT.1 (ref. [28]).

253. I consider this position adequate for Step 2 of GDA in advance of the RP developing UK radiological criteria for direct comparison with Target 4 in future. The RP has committed to doing this for a future PCSR under FAP item 15.5-32 of ref. [73]. Furthermore, as previously mentioned, the RP has produced a specification for a UK safety case manual (ref. [97]) covering UK radiological criteria for use in producing a PCSR. This gives me sufficient confidence it can develop UK radiological criteria which will provide that future comparison.

4.3.8. Verification and Validation of Codes

254. It is my expectation that methods used to perform deterministic analysis supporting safety case claims are adequately verified and validated. My expectations are informed by ONR's SAPs AV.1 to 6 (excluding AV.4) (ref. [28]) and NS-TAST-GD-042 (ref. [29]). For BWRX-300, the main codes deployed for all deterministic analyses are TRACG, GOTHIC and MAAP. In my assessment, I have relied heavily on reviews of the codes from both the US NRC and CNSC and previous assessment performed by ONR on the UK ABWR GDA. In this section, I summarise the work performed and why I consider it relevant to my assessment.

TRACG

255. The RP has used TRACG for the steady state and transient analysis of all reactor faults. TRACG is a 3-dimensional reactor kinetics and 2-phase thermal hydraulics code which has been used by the RP for generations of BWRs covering BWR/2 to BWR/6. In particular, the US NRC approved it for use for ESBWR (Economic Simplified Boiling Water Reactor) in supporting its design certification, noting ESWBR also relies solely on natural coolant circulation. Since then, the US NRC have undertaken a review of the RP's use of TRACG for BWRX-300. This has been done against standards and guidance which I consider comparable in purpose to ONR's (see Appendix 3 – Findings by other regulators).

256. In its review, US NRC accepted the RP's reliance on previous validation evidence for ESBWR and natural coolant circulation (and considerations of important phenomena) based on evidence from an impact review of the design differences between BWRX-300 and ESBWR. This evidence is summarised in section 15.5.1.2.1 of Chapter 15.5 (ref. [18]). This includes tests undertaken at Berkeley, University of California which validates the TRACG modelling of natural heat transfer relating to steam condensation in tubes and the RP's own qualification tests undertaken using a full-scale Isolation Condenser (IC) prototype known as PANTHERS.

257. ONR has previously assessed the application of TRACG for the ABWR (ref. [66]). This concluded: "I judge both the code and its use to be consistent with my expectations (as established by the SAPs) and I have no issues with its appropriateness for the UK ABWR GDA.". This, coupled with the US NRC's reviews covering the extra natural coolant circulation aspects, provides me with confidence that it is adequately validated for use for the BWRX-300. I have, therefore, chosen not to sample the validation evidence in any detail. I share this position with the PSA inspector (see ref. [86]).

GOTHIC

258. GOTHIC is a well-established multipurpose containment code which is commonly applied to containment thermal hydraulics analysis of light water reactors. The GOTHIC code has been approved for use for several applications by the US NRC.

259. The RP has used TRACG to model the mass and energy discharge from LOCAs into containment. To model the consequent thermal hydraulic impacts, the RP has used GOTHIC. This is a 2-phase heat transfer and fluid flow code which has been approved by US NRC for use for containment analysis for many operating reactors and new reactor designs. For BWRX-300, the US NRC and the CNSC have both individually then jointly reviewed the combined use of TRACG/GOTHIC to model containment impact and the performance of the PCCS. This has been done against standards and guidance which I consider comparable in purpose to ONR (see Appendix 3 – Findings by other regulators).

260. In particular, as detailed in Appendix 3 – Findings by other regulators, the US NRC have undertaken an independent confirmatory analysis using different analytical models (TRACE and MELCOR). They have also benchmarked GOTHIC predictions against test data from the Carolina Virginia Tube Reactor (CVTR). This is a facility used for conducting large scale tests to provide experimental information on the response of containment structures to severe events.

MAAP

261. The MAAP computer code has been used to perform deterministic analysis of the severe accident sequences.

262. Assessment of the verification and validation (V&V) of MAAP was conducted by ONR during the GDA for the ABWR. This concluded MAAP was suitable for use for the modelling of severe accidents for ABWR (ref. [101]). Since severe accident phenomena are common amongst BWRs, I have taken credit for this assessment, choosing not to sample validation evidence. I share this position with the PSA inspector (see ref. [86]).

Summary of validation of computer codes

263. Although I have not performed a detailed review of the validation evidence, I have gained sufficient confidence through ONR's previous assessment of the codes, the US NRC and CNSC reviews of the application of TRACG, GOTHIC and MAAP, that there would be no significant shortfalls against my expectations for validation of computer codes, as set out in SAPs AV.1 to 6 (excluding AV.4) (ref. [28]). Based on this, I judge that the TRACG, GOTHIC and MAAP codes are suitable for use for Step 2 of GDA.

4.3.9. Practical Elimination

264. Informed by SSG-88 (ref. [57]), it is my expectation that the safety case provides arguments for why sequences that have the potential to lead to large or early release, can be considered practically eliminated. For Step 2 of GDA, the RP has identified a range of events or conditions and the associated relevant DL provisions which are claimed and then argued to achieve practical elimination (see Table C-1 of Appendix C of ref. [22]).

265. The RP's methodology takes both a deterministic and probabilistic approach to the demonstration of practical elimination.

266. The RP's arguments related to practical elimination cover events such as gross RPV rupture as well as sequences involving severe accident phenomena. These arguments rely on DL provisions which include robust design to prevent accidents, as well as design basis safety measures and severe accident safety features as appropriate.

267. Further assessment of the DSA and PSA along with assessment of other areas (such as hazards and structural integrity) as all committed to under the

various relevant plans[18] would be required for ONR to form a judgement on whether the BWRX-300 design practically eliminates sequences that have the potential to lead to a large or early release. However, notwithstanding the gaps and plans identified in this report, I judge that the BWRX-300 design is based on the concept of DiD, and that the RP's approach to the demonstration of practical elimination aligns well with SSG-88 (ref. [57]), and have confidence that a future case for practical elimination could be made.

4.3.10. ALARP

4.3.10.1. Design Approach

268. Chapter 27 of the PSR (ref. [24]) states that the BWRX-300 is GE-Vernova Hitachi's tenth generation of BWR since 1955. While earlier generations focused on improving performance culminating with the ABWR, later generations have focused on simplifying reactor systems and containment design. The BWRX-300 design goal is to reduce cost and hasten deployment by down-scaling the BWR design in a way that eases construction and reduces operating burden, whilst achieving safety levels. The BWRX-300 seeks to achieve this goal with the following choice of features:

- Large passive cooling condensers which eliminate the need for SRVs and which, along with the integral RIVs, minimise potential steam releases into containment, enabling a simple 'dry' containment design;
- A tall RPV with a large 'chimney' section which allows generous core coverage and high natural circulation flow. This avoids reliance on active systems while enabling the use of existing GNF2 fuel and other core design aspects including the FMCRDs; and
- A below ground construction minimises the adverse impact of a tall RPV on fuel storage and transport arrangements.

269. From my assessment, I consider the BWRX-300 design generally meets my expectations of the ONR SAPs relating to the Fault Studies and Severe Accident Analysis topic (as listed in Appendix 1) and I have found no fundamental safety shortfalls. I have found that the RP's approach to fault and sequence identification is adequate, the RP has identified measures to protect against those faults, the analysis has been performed conservatively (as appropriate), the radiological consequences are likely to be within numerical targets, and the codes are adequately validated for use. I have also found that the RP's approach to categorisation of safety functions and classification of SSCs for the reactor is adequate. On this basis, I consider

[18] Including FAP items 15.5-30, 15.6-42, 15.5-29 and 15.7-63 (ref. [73]) plus resolution plan (ref. [80])

the BWRX-300 design provides a good foundation for the RP to demonstrate risks reduced ALARP within a future safety case.

270. The RP has given me further confidence by setting out the 'ALARP Evaluation' process it would use to demonstrate that risks are reduced ALARP. This process is described in ref. [24] and comprises 3 phases which incorporate risk assessment and design decision making processes:

- Phase 1: Holistic review of BWRX-300
- Phase 2: Specific review of potential improvements (options)
- Phase 3: Holistic evaluation of the ALARP position

271. I note the RP has already undertaken a Phase 1 ALARP review in parallel to the Step 2 of GDA. This has involved identifying gaps against RGP (including those originating from ONR's findings) to be taken forward as FAP items for Phase 2 ALARP review. I consider this process to be in keeping with meeting the safety case characteristics which concern ALARP as set down in paragraph 102 of SC.4 of the SAPs (ref. [28]). I am therefore confident the RP could provide an ALARP demonstration within a future safety case.

272. I have found several events and sequences concerning large un-isolated and unisolable LOCAs that require resolution for a future safety case under Resolution Plan, ref. [80]. However, I consider there are two sequences which would need specific attention to demonstrate their risks are reduced ALARP. These are 'Non-Isolated ICS LOCAs' and 'Failure to Scram' sequences (see section 4.3.3.3). In my opinion, the RP would have to progress analysis of these sequences under the FAP items described in the following sections to support ALARP demonstration for a future safety case (FAP items 15.5-404, 15.5-29 and 15.5-406 of ref. [73]).

4.3.10.2. Non-Isolated ICS LOCAs

273. As stated previously, the ICS plays a principal role in heat removal for both intact circuit faults and LOCAs. There are competing safety aspects to the ICS. For LOCAs on the ICS pipework, it is important that the break is isolated. However, the greater the provision made to isolate the ICS, the more likely inadvertent isolation of the ICS may become.

274. I have found that the RP has made the following design choices which prioritise the availability of the ICS over its isolation protection:

- only the PPS can close the ICS RIVs (they cannot be closed by the DPS)
- ICS RIVs fail 'as is' (which means they would remain open)
- ICS RIVs can only be manually closed from the SCR (not the CCR)

- ICS RIVs are mechanically inhibited from closing when the associated ICS train is in service

- no more than one ICS train can be isolated at any time (as vetoed by mechanical means)

275. In my opinion, the RP has not adequately justified exclusion of a break on the ICS pipework with failure of that ICS pipework to be isolated, from either design basis or DEC-A analysis. It is my opinion the design has left these sequences short of provision and that a future BWRX-300 safety case should provide further analysis to support an ALARP demonstration.

276. In response to RQ-01770 (ref. [78]) the RP has provided the assurances below:

- Firstly, the RP has already undertaken preliminary analysis of the non-isolated ICS LOCA scenario, in which credit is placed on the control rod drive hydraulic sub-system. This analysis indicates no fuel overheating, implying that serious radiological consequences can be avoided. The RP's completion of this analysis is tracked by RO-BWRX300-004 (ref. [79]), noting this RO also covers analysis of other LOCAs (including non-unisolable LOCAs involving breaks at the RPV/RIV connection). In response to RO-BWRX300-004 (ref. [79]), the RP have produced a Resolution Plan (ref. [80]);

- Secondly, the RP's PSA has assessed the comparative contribution of non-isolated ICS LOCA sequences to CDF (Core Damage Frequency) to be very low, to the satisfaction of the PSA Inspector (see ref. [102]); and

- Thirdly, the RP has committed to considering potential safety improvements to the actuation of the ICS isolation during Phase 3 of the ALARP evaluation for future PCSR under FAP 15.5-404 item of ref. [73].

277. On this basis, I am content that no fundamental shortfalls exist with the design at Step 2 and am confident a future BWRX-300 safety case would be able to provide an ALARP demonstration against Non-isolated ICS LOCAs.

4.3.10.3. Failure to Scram

278. I have found that the RP's submitted fault analysis has not covered sequences involving a failure to scram (e.g. by mechanical failure to insert rods).

279. In response to RQ-01875 (ref. [82]), the RP has claimed the probability of failure on demand of the Hydraulic Scram to be $2x10^{-6}$ pfd (see section 4.3.3.2). The RP has claimed the joint probability of failure on demand of both the Hydraulic Scram and motorised CR run-in to be $2.7x10^{-7}$ pfd.

280. I consider the joint claim against CCF of both systems to be ambitious carrying significant uncertainty. In particular, I consider the claim to be

challenging to the expectations related to providing independence between levels of defence in depth (EKP.3), having two diverse means of shutdown (ECR.3), and claiming large reliability figures (EDR.3), noting both systems commonly rely on control rods. Moreover, the BWRX-300 potentially falls short of Requirement 46 of SSR-2/1 (ref. [55]), in which two independent means of shutdown are required.

281. Therefore, I judge that the RP has not adequately demonstrated that the sequence should be excluded from the design basis or design extension conditions with limited core damage. I, therefore, expect that this sequence should be further analysed and diverse provisions claimed, or justification should be provided for why the two means are suitably diverse and the combined CCF claim justified.

282. The BWRX-300 design does include a diverse means of shutdown (BIS) but the RP has not claimed it for DBAs or DEC-A sequences, nor has the RP demonstrated its effectiveness in meeting DEC-A acceptance criteria. Furthermore, since the BIS has been presented as a single train Class 3 system which is manually actuated, it is not apparent it would be capable of doing this nor sufficiently reliable in keeping with reducing risks ALARP (in the context of high reliability claims on the Hydraulic Scram).

283. The RP has acknowledged the gap against ‘failure to scram’ and has committed to further work concerning the BIS under FAP item 15.5-29 of ref. [73]. This identifies the gap against the expectations of EKP.3, ECR.3 and EDR.3 of SAPs (ref. [28]) and has set out a need for the future PCSR to confirm the design status of the BIS and provide a demonstration of its functional capability and reliability if needed. I am therefore content the RP has both identified the gap and made the appropriate commitment. I am also content that, in response to RQ-01875 (Ref. [82]), the RP has further committed to covering reliability improvements to the BIS during Phase 3 of the ALARP evaluation for future PCSR under FAP 15.5-406 item of ref. [73].

284. Moreover, since the start of Step 2 of GDA, the BIS has undergone further design development in support of the BWRX-300 safety case in Canada, where the CNSC have granted the future operator a Licence to Construct BWRX-300 at Darlington[19] (see also Appendix 3 – Findings by other regulators). In response to RQ-02306 (ref. [103]), the RP has provided additional information concerning this development which would be expected to apply to the UK.

285. Ref. [103] describes how the developed BIS design features automatic initiation and that deterministic analysis (EX-DSA) has been progressed. This analysis demonstrates that the developed BIS design can act in conjunction with the UPR and containment venting to safely shutdown the

[19] Ontario Power Generation (OPG) are the future operator of the BWRX-300 at Darlington, known as the DNNP (Darlington New Nuclear Project), where GVHA provide safety case support

reactor in failure to scram sequences before DEC-A acceptance criteria is exceeded and core melt can occur. Therefore, while BIS, UPR and containment vent are all allocated to DL4b (normally associated with controlling severe accidents), this gives me confidence they could collectively fulfil a duty to prevent a severe accident and provide a feasible ALARP measure for safe shutdown. On this basis, I am confident a future BWRX-300 safety case for the UK would be able to provide an ALARP demonstration against failure to Scram sequences.

Seismic

286. The response to RQ-02306 (ref. [103]) confirms BIS to be rated “non-seismic”. Meanwhile, certain parts supporting motorised CR run-in are also rated “non-seismic” (see ref. [104]). If both were lost in an Operating Basis Earthquake (OBE)[20], then it would place sole reliance on Hydraulic Scram. Since the OBE is a frequent hazard, this could once again challenge expectation for an alternative means of shutdown against FA.6, EKP.3, ECR.3 and EDR.3 of SAPs (ref. [28]).

287. However, the OBE has not been defined for Step 2 of GDA. Instead, the OBE is considered a site-specific hazard to be addressed by future PCSR under FAP item PSR15.8-144 (ref. [73]). This approach is considered appropriate by the External Hazards Inspector (ref. [105]). Once defined for PCSR, then an ALARP review against the OBE would follow, covering alternative shutdown means (noting ALARP evaluation of BIS is specifically covered under FAP 15.5-406 item of ref. [73]).

288. Meanwhile, I judge there to be no fundamental safety shortfall for the following reasons:

- The response to RQ-02127 (ref. [106]) confirms that all parts of the motorized CR run-in which are rated “non-seismic” (including power supplies) are all contained within the reactor building. Since this building is qualified to the DBE with secondary effects addressed, it would support an option to qualify those parts against the less demanding OBE in future; and

- Moreover, while an OBE is considered a frequent hazard, it is conservatively defined on the basis that it arises no more than once during operating life. Therefore, even if alternative means could not be completely qualified to the OBE level, I would still expect them to be capable of some minimum (or limited) level of seismic resilience and risk reduction to low levels to be achievable.

[20] The OBE is a more moderate seismic event than the DBE expected to occur once during operating life

289. To conclude, while I consider the high reliability claims of the Hydraulic Scram would require more detailed assessment, I do not consider the omission of seismic qualification requirements for the alternative shutdown means to present a fundamental safety shortfall.

4.3.10.4. Conclusions Related To ALARP

290. From a Fault Studies and Severe Accident Analysis point of view, the BWRX-300 design includes safety measures to protect or mitigate identified initiating events and sequences.

291. The RP's process for ALARP decision making process is embedded in the design process, and is aligned with my expectations, informed by NS-TAST-GD-006 (ref. [29]).

292. I am content that the RP have acknowledged the shortfall in provision against ICS LOCAs, have already undertaken preliminary analysis of the consequences giving me confidence they can be effectively mitigated, and have committed to the further work needed to demonstrate residual risks reduced ALARP.

293. I am content that the RP have acknowledged the potential shortfall in provision against failure to scram, have already taken reasonably practicable steps to develop a means using BIS, and have committed to the further work needed to demonstrate residual risks ALARP, including seismic considerations.

4.3.11. Approach to Documenting Fault Analysis

294. Informed by SSG-61 (ref. [58]), I expect the RP to document its safety analysis within Chapter 15 of the PSR covering AOOs, DBAs and DECs including severe accidents. While I consider Chapter 15 (ref. [18]) adequately documents AOOs, DBAs and DEC-A analysis and safety criteria, I have found it has not adequately presented DEC-B analysis (noting this was recognised by the RP under FAP item PSR15-4 of ref. [73]).

295. Instead, as described in section 4.2, my assessment of DEC-B analysis has relied on supplementary information submitted during the Step 2 GDA. This supplementary information is described in section 4.3.5 and includes a response to an RQ (ref. [96]).

296. Aside from the above and informed by ONR's SAPs, I have compared the RP's safety case submission against a shortlist of safety case characteristics listed in paragraphs 100-102 under SAP SC.4 (ref. [28]). I consider the RP's safety case submission to have met fundamental characteristics expected for Step 2.

5. Conclusions

297. This report presents the Step 2 Fault Studies & Severe Accident Analysis assessment for the GDA of the BWRX-300 design. The focus of my assessment in this step was towards the fundamental adequacy of the design and safety case. I have assessed the SSSE chapters and relevant supporting documentation provided by the RP to form my judgements. I targeted my assessment, in accordance with my assessment plan (ref. [32]), at the content of most relevance to Fault Studies & Severe Accident Analysis against the expectations of the ONR's SAPs, TAGs and other guidance which ONR regards as relevant good practice, such as IAEA standards (ref. [56]).

298. My assessment scope has largely been limited to power operations of the BWRX-300. Based upon my assessment, I have concluded the following:

- The RP's approach to defence in depth and safety categorisation and classification is adequate;
- The RP's approach to fault analysis provides a robust demonstration of multiple layers of defence in depth;
- The RP's methodology for initiating event and sequence identification is adequate. However, I have identified some initiating events and sequences that require further justification for exclusion, a demonstration of protection against them, or design modifications to provide adequate protection. These concern large LOCAs and the RIVs as well as high reliability claims placed on Scram systems and on the ICS. For all these sequences, I am content there are appropriate Forward Action Plans and have confidence the RP could make an adequate case in future;
- For design basis accident and design extension conditions with limited fuel damage sequences that the RP has identified, the deterministic analysis adequately demonstrates that the safety measures are sufficient to meet the RP's safety criteria;
- The RP's approach to severe accident analysis is appropriate in determining sufficient severe accident safety features, and the safety features feasibly prevent or mitigate appropriate phenomena;
- The RP has yet to apply its fault analysis approach to non-reactor faults, start-up and shutdown faults. However, the RP have presented some preliminary analysis which provides me with confidence in the methodologies that will be applied. I am content there is a Forward Action Plan covering these faults and I have confidence that a future safety case could be made;

- No radiological consequence assessment has been undertaken, to date. However, since decoupled criteria are met for design basis faults, and based on the design of the BWRX-300, I do not consider that this will be particularly challenging at a later stage;

- The computer codes used to underpin design basis and severe accident analysis are adequately validated for use;

- A overall demonstration of practical elimination has not been provided, to date. However, the RP's approach to defence in depth and the deterministic analysis of safety measures provided for design basis and severe accident analysis provide confidence that an adequate case can be made in the future; and

- The RP's adoption of good practice to fault analysis and design development provides confidence that a demonstration of ALARP will be achievable at a later stage subject to completing further work identified in its Forward Action Plans.

299. During my assessment, I have raised one Regulatory Observation regarding Loss of Coolant Accident sequences that I judge should be further assessed and demonstrated to be adequately protected against.

300. Overall, based on my assessment, and subject to the provision and assessment of suitable and sufficient supporting evidence in either a future Step 3 GDA or during site specific activities, I have not identified any fundamental safety shortfalls which could prevent ONR permissioning the construction of a power station based on the generic BWRX-300 design.

6. References

[1] GE-Hitachi, NEDC-34162 BWRX-300 UK GDA - Safety Security Safeguards Environment Summary, Rev C, 15 July 2025, ONRW-2019369590-22495.

[2] GE-Hitachi, NEDO-34169 PSR Chapter 1 Introduction, Rev B, 11 July 2025, ONRW-2019369590-22414.

[3] GE-Hitachi, NEDO-34164 Chapter 2 Site Characteristics, Rev B, 15 July 2025, ONRW-2019369590-22496.

[4] GE-Hitachi, NEDO-34165 Chapter 3 - Safety Objectives and Design Rules for SSCs, Rev C, 15 July 2025, ONRW-2019369590-22497.

[5] GE-Hitachi, NEDC-34166P BWRX-300 UK GDA Chapter 4 - Reactor, Rev C, 15 July 2025, ONRW-2019369590-22500.

[6] GE-Hitachi, NEDO-34167 BWRX-300 UK GDA Chapter 5 - Reactor Coolant System and Associated Systems, Rev B, 11 July 2025, ONRW-2019369590-22393.

[7] GE-Hitachi, NEDO-34168 BWRX-300 UK GDA Chapter 6 - Engineered Safety Features, Rev B, 11 July 2025, ONRW-2019369590-22395.

[8] GE-Hitachi, NEDO-34169 BWRX-300 UK GDA Chapter 7 - Instrumentation and Control, Rev B, 11 July 2025, ONRW-2019369590-22414.

[9] GE-Hitachi, NEDO-34170 BWRX-300 UK GDA Chapter 8 - Electrical Power, Rev C, 15 July 2025, ONRW-2019369590-22501.

[10] GE-Hitachi, NEDO-34171 BWRX-300 UK GDA Chapter 9A - Auxiliary Systems, Rev B, 11 July 2025, ONRW-2019369590-22415.

[11] GE-Hitachi, NEDC-34172 BWRX-300 UK GDA Chapter 9B - Civil Structures, Rev B, 11 July 2025, ONRW-2019369590-22416.

[12] GE-Hitachi, NEDO-34173 BWRX-300 UK GDA Chapter 10 - Steam Power Conversion, Rev B, 11 July 2025, ONRW-2019369590-22417.

[13] GE-Hitachi, NEDO-34178 BWRX-300 UK GDA Chapter 15 - Safety Analysis (Fault Studies, PSA, Hazard Assessment), Rev B, 11 July 2025, ONRW-2019369590-22392.

[14] GE-Hitachi, NEDC-34179P BWRX-300 UK GDA Chapter 15.1 - Safety Analysis - General Considerations, Rev B, 15 July 2025, ONRW-2019369590-22391.

[15] GE-Hitachi, NEDO-34180 BWRX-300 UK GDA Chapter 15.2 - Safety Analysis Identification Categorization and Grouping, Rev B, 15 July 2025, ONRW-2019369590-22505.

[16] GE-Hitachi, NEDO-34181 BWRX-300 UK GDA Chapter 15.3 - Safety Analysis Safety Objectives and Acceptance Criteria, Rev C, 15 July 2025, ONRW-2019369590-22506.

[17] GE-Hitachi, NEDO-34182 BWRX-300 UK GDA - Chapter 15.4 - Safety Analysis Human Actions, Rev B, 15 July 2025, ONRW-2019369590-22507.

[18] GE-Hitachi, NEDC-34183P BWRX-300 UK GDA Chapter 15.5 - Deterministic Safety Analysis, Rev B, 15 July 2025, ONRW-2019369590-22509.

[19] GE-Hitachi, NEDO-34184 BWRX-300 UK GDA Chapter 15.6 - Probabilistic Safety Assessment, Rev B, 15 July 2025, ONRW-2019369590-22508 .

[20] GE-Hitachi, NEDC-34185 BWRX-300 UK GDA Chapter 15.7 - Internal Hazards, Rev B, 15 July 2025, ONRW-2019369590-22510.

[21] GE-Hitachi, NEDO-34186 BWRX-300 UK GDA Chapter 15.8 - Safety Analysis - External Hazards, Rev B, 15 July 2025, ONRW-2019369590-22511.

[22] GE-Hitachi, NEDO-34187 BWRX-300 UK GDA Chapter 15.9 - Summary of Results of the Safety Analyses, Rev B, 15 July 2025, ONRW-2019369590-22512.

[23] GE-Hitachi, NEDO-34194 BWRX-300 UK GDA Chapter 22 Structural Integrity of Metallic System Structures and Components, Rev B, 3 July 2025, ONRW-2019369590-22202.

[24] GE-Hitachi, NEDO-34199 BWRX-300 UK GDA Chapter 27 - ALARP Evaluation, Rev B, 11 July 2025, ONRW-2019369590-22420.

[25] GE-Hitachi, NEDC-34154P BWRX-300 UK GDA Design Reference Report, Revision 3, April 2025, ONRW-2019369590-20194.

[26] ONR, Guidance on Mechanics of Assessment, NS-TAST-GD-096, Issue 1.2, December 2022. www.onr.org.uk/operational/tech_asst_guides/index.htm.

[27] ONR, Risk-informed and targeted engagements (RITE), ONR-RD-POL-002, Issue 2, May 2024. (Record ref. 2024/16720).

[28] ONR, Safety Assessment Principles for Nuclear Facilities (SAPs), 2014 Edition, Revision 1, January 2020. www.onr.org.uk/saps/saps2014.pdf.

[29] ONR, Technical Assessment Guides. www.onr.org.uk/operational/tech_asst_guides/index.htm.

[30] ONR, Guidance on the Production of Reports for Permissioning and Assessment, NS-TAST-GD-108, Issue No. 2, December 2023, (Record ref. 2022/71935).

[31] ONR, Guidance to Requesting Parties on the Generic Design Assessment (GDA) process for safety and security assessments of new Nuclear Power Plants (NPP), ONR-GDA-GD-006, Issue 1, August 2024 (Record ref. 2024/34844).

[32] ONR, Step 2 Fault Studies Assessment Plan for the Generic Design Assessment of the GE Hitachi BWRX-300 (plus Severe Accident Analysis), Issue 1, ONR-2126615823-4253.

[33] ONR, Generic Design Assessment of the BWRX-300 - Step 2 Summary Report, Revision 1, December 2025, ONRW-2019369590-21328.

[34] GE-Hitachi, NEDC-34174P BWRX-300 UK GDA Chapter 11 - Management of Radioactive Waste, Rev B, 3 July 2025, ONRW-2019369590-22201.

[35] GE-Hitachi, NEDC-34175P BWRX-300 UK GDA Chapter 12 - Radiation Protection, Rev B, 3 July 2025, ONRW-2019369590-22203.

[36] GE-Hitachi, NEDO-34176 BWRX-300 UK GDA Chapter 13 - Conduct of Operations, Rev B, 15 July 2025, ONRW-2019369590-22502.

[37] GE-Hitachi, NEDC-34177P BWRX-300 UK GDA Chapter 14 - Plant Construction and Commissioning, Rev B, 15 July 2025, ONRW-2019369590-22503.

[38] GE-Hitachi, NEDC-34188P BWRX-300 UK GDA Chapter 16 - Operational Limits Conditions, Rev B, 15 July 2025, ONRW-2019369590-22513.

[39] GE-Hitachi, NEDO-34189 BWRX-300 UK GDA Chapter 17 - Management for Safety and Quality Assurance, Rev 1 , 15 July 2025, ONRW-2019369590-22514.

[40] GE-Hitachi, NEDO-34190 BWRX-300 UK GDA Chapter 18 - Human Factors Engineering, Rev B, 15 July 2025, ONRW-2019369590-22515.

[41] GE-Hitachi, NEDO-34191 BWRX-300 UK GDA Chapter 19 - Emergency Preparedness and Response, Rev B, 15 July 2025, ONRW-2019369590-22516.

[42] GE-Hitachi, NEDO-34192 BWRX-300 UK GDA Chapter 20 Environmental Aspects, Rev B, 11 July 2025, ONRW-2019369590-22394.

[43] GE-Hitachi, NEDO-34193 BWRX-300 UK GDA Chapter 21 Decommissioning and End of Life Aspects, Rev B, 11 July 2025, ONRW-2019369590-22418.

[44] GE-Hitachi, NEDO-34195P BWRX-300 UK GDA Chapter 23 Reactor Chemistry, Rev C, 11 July 2025, ONRW-2019369590-22419.

[45] GE-Hitachi, NEDO-34196P BWRX-300 UK GDA Chapter 24 - Conventional Safety and Fire Safety Summary Report, Rev B, 3 July 2025, ONRW-2019369590-22204.

[46] GE-Hitachi, NEDO-34197 BWRX-300 UK GDA Chapter 25 - Security, Rev B, 3 July 2025, ONRW-2019369590-22205.

[47] GE-Hitachi, NEDC-34198P BWRX-300 UK GDA Chapter 26 Spent Fuel Management, Rev B, 11 July 2025, ONRW-2019369590-22401.

[48] GE-Hitachi, NEDO-34200 BWRX-300 UK GDA Chapter 28 Safeguards, Rev B, 3 July 2025, ONRW-2019369590-22206.

[49] GE-Hitachi, NEDC-34148P, Scope of Generic Design Assessment, Revision 2, September 2024, ONRW-2019369590-13525.

[50] GE-Hitachi, NEDO-34087, BWRX-300 UK Generic Design Assessment Master Document Submission List (MDSL), Revision 19, November 2025, ONRW-2019369590-25137.

[51] IAEA, Safety Standards. www.iaea.org.

[52] IAEA, Nuclear Security series. www.iaea.org.

[53] WENRA, Safety Reference Levels for Existing Reactors 2020, February 2021. www.wenra.eu.

[54] WENRA, Safety Objectives for New Nuclear Power Plants and WENRA Report on Safety of new NPP designs - RHWG position on need for revision, September 2020. www.wenra.eu.

[55] IAEA Safety Standards, Safety of Nuclear Plants: Design, Specific Safety Requirements, No. SSR-2/1 (Rev.1). www.iaea.org.

[56] IAEA Safety Standards, Deterministic Safety Analysis for Nuclear Power Plants, Specific Safety Guide No. SSG-2 (Rev 1). www.iaea.org.

[57] IAEA Safety Standards, Design Extension Conditions and the Concept of Practical Elimination in the Design of Nuclear Power Plants, Specific Safety Guide No. SSG-88. www.iaea.org.

[58] IAEA Safety Standards, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61. www.iaea.org.

[59] GE-Hitachi, 006N5064 BWRX-300 Safety Strategy Specification, Revision 6, ONRW-2019369590-18450.

[60] GE-Hitachi, NEDC-34145P BWRX-300 UK GDA Conventional Safety Strategy (Methods), Revision 1, August 2024, ONRW-2019369590-13984.

[61] GE-Hitachi, NEDC-34142P BWRX-300 UK GDA Security Design Assessment Strategy, Revision 0, May 2024, ONRW-2019369590-9733.

[62] GE-Hitachi, NEDC-34140P BWRX-300 UK GDA Safety Case Development Strategy, Revision 0, June 2024, ONRW-2019369590-10299.

[63] GE-Hitachi, 005N9461 BWRX-300 Structures, Systems, and Components (SSCs) Safety Classification, Revision 4, ONRW-2019369590-7930.

[64] ONR, Delivery Strategy for the Generic Design Assessment of the GE Hitachi BWRX-300, Issue 1, 17 July 2024, ONRW-2019369590-11067.

[65] ONR, Generic Design Assessment, Assessment of Reactors, UK Advanced Boiling Water Reactor, https://www.onr.org.uk/generic-design-assessment/assessment-of-reactors/uk-advanced-boiling-water-reactor-uk-abwr/.

[66] ONR, Step 4 Assessment of Fault Studies for the ABWR, ONR-NR-AR-17-016 Revision 0, December 2017 (Record ref. 2017/98169).

[67] ONR, Generic Design Assessment of the BWRX-300 - Step 2 Assessment of Fuel and Core Design, December 2025, ONRW-2126615823-7941 .

[68] ONR, Technical Assessment Guide, Categorisation of safety functions and classification of structures, systems and components (SSCs), NS-TAST-GD-094, Issue 2.1, May 2025, www.onr.org.uk/operational/tech_asst_guides/index.htm.

[69] IAEA Safety Standards, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide, No. SSG-30. www.iaea.org.

[70] GE-Hitachi, 005N3558 BWRX-300 Fault Evaluation, Revision 3, ONRW-2019369590-14830.

[71] ONR, Generic Design Assessment of the Rolls Royce SMR - Step 2 Assessment of Fault Studies, June 2024, ONRW-2126615823-2793.

[72] GE-Hitachi, NEDC-34161P Comparison of BWRX-300 Approach to Categorisation & Classification with UK Expectations, Revision 0, 6th September 2024, ONRW-2019369590-14008.

[73] GE-Hitachi, NEDC-34274P Forward Action Plan, Revision 2, July 2025, ONRW-2019369590-22522.

[74] GE-Hitachi, 006N9004 BWRX-300 Deterministic Safety Analysis Performance Requirements, Revision 2, ONRW-2019369590-17679.

[75] GE-Hitachi, Generic Design Assessment of the BWRX-300 – Step 2 assessment of Internal Hazards, December 2025, ONRW-2126615823-8059.

[76] GE-Hitachi, Submission of BWRX-300 UK GDA Step 2 RQ-01870 Response, 04 April 2025, ONRW-609516046-1332.

[77] GE-Hitachi, Submission of BWRX-300 UK GDA, RQ-01763 Full Response, 14 March 2025, ONRW-609516046-1070.

[78] GE-Hitachi, Submission of BWRX-300 UK GDA, Response to Regulatory Query RQ-01770, Full Response, 16 May 2025, ONRW-2019369590-20778.

[79] ONR, RO-BWRX300-004 - Safety Case for un-isolable and non-isolated pipe-breaks larger than 19mm, 17 July 2025, ONRW-2126615823-7940.

[80] GE-Hitachi, Submission of BWRX-300 UK GDA RO-BWRX300-004 Resolution Plan, 11 September 2025, ONRW-2126615823-8637.

[81] GE-Hitachi, Submission of BWRX-300 UK GDA Step 2 RQ-01761 Response, 25 March 2025, ONRW-609516046-1199.

[82] GE-Hitachi, Submission of BWRX-300 UK GDA GEH Response to Regulatory Query RQ-01875, 2 May 2025, ONRW-2019369590-20339.

[83] ONR, Generic Design Assessment of the BWRX-300 - Step 2 Assessment of Mechanical Engineering, December 2025, ONRW-2126615823-7759.

[84] ONR, Generic Design Assessment of the BWRX-300 – Step 2 Assessment of Chemistry, December 2025, ONRW-2126615823-770.

[85] GE-Hitachi, 008N9751 BWRX-300 Probabilistic Safety Assessment Summary Report for UK Generic Design Assessment (GDA) Review, Revision 1, 2025, ONRW-2019369590-18322.

[86] ONR, Generic Design Assessment of the BWRX-300 - Step 2 Assessment of the PSA, December 2025, ONRW-2126615823-7783.

[87] ONR, Generic Design Assessment of the BWRX-300 - Step 2 Assessment of Civil Engineering, December 2025, ONRW-2126615823-8118.

[88] GE-Hitachi, Submission of BWRX-300 UK GDA, Regulatory Query RQ-01768 Full Response, 10 April 2025, ONRW-609516046-1413.

[89] ONR, Contact Record ID: ONR-NR-CR-24-769 Level 4 Fault Studies/SAA Cross-Topic Meetings – LOCAs & Over-Pressures – 21st & 27th February 2025, ONRW-2019369590-18426.

[90] GE-Hitachi, Enclosure 1 BWRX-300 Full Power Internal Event Severe Accident Analysis, BWRX-300 UK GDA, DBR-0078539, Revision A, ONRW-2019369590-21352.

[91] GE-Hitachi, Enclosure 2 Darlington New Nuclear Project Severe Accident Analysis Methodology, BWRX-300 UK GDA, 007N3122, Revision 2, ONRW-2019369590-21354.

[92] GE-Hitachi, Enclosure 3 BWRX-300 Darlington New Nuclear Project, BWRX-300 UK GDA, 007N6885, Revision B, ONRW-2019369590-21351.

[93] CNSC, Deterministic Safety Analysis, REGDOC-2.4.1, CNSC file 5298002, May 2014.

[94] CNSC, Design of Reactor Facilities: Nuclear Power Plants, REGDOC-2.5.2, CNSC file 4438515, May 2014.

[95] EPRI, EPRI MAAP5 – Modular Accident Analysis Program for LWR Power Plants, Transmittal Document for MAAP5 Code Revision MAAP 5.06, Electric Power Research Institute, 2021.

[96] GE-Hitachi, Submission of BWRX-300 UK GDA, Response to Regulatory Query RQ-01769, Full Response, 16 May 2025, ONRW-2019369590-20776 .

[97] GE-Hitachi, NEDC-34357P BWRX-300 UK Generic Design Assessment (GDA) Safety Case Manual Specification, Revision A, April 2025, ONRW-2019369590-20154.

[98] GE-Hitachi, Submission of BWRX-300 UK GDA, Regulatory Query RQ-01776 Full Response, 29 April 2025, ONRW-609516046-1603.

[99] NRC, Alternative Fuel Handling Accident Transport Methodology, NRC file ML19248C668, https://www.nrc.gov/docs/ML1924/ML19248C668.pdf.

[100] ONR, Contact Record ID: ONR-NR-CR-24-886 Level 4 Fault Studies and Severe Accident Meetings - 'DBA Exclusions' & Severe Accident - 21st & 27th March 2025, ONRW-2019369590-20423.

[101] ONR, Step 4 Assessment of Severe Accident Analysis for the UK ABWR, ONR-NR-AR-17-015 Revision 0, December 2017, (Record ref. 2017/98159).

[102] GE-Hitachi, Meeting Notes, G-MTG-L4-PSA-0010, BWRX-300 UK Generic Design Assessment, Subject "PSA Step 2 - ICS LOCA detection query and general process discussion", 25th April 2025, ONRW-2019369590-20092.

[103] GE-Hitachi, Submission of BWRX-300 UK GDA - Response to Regulatory Query (RQ) 02306, 11 September 2025, ONRW-2019369590-23831.

[104] ONR, Generic Design Assessment of the BWRX-300 - Step 2 Assessment of the Electrical Engineering, December 2025, ONRW-2126615823-7654.

[105] ONR, Generic Design Assessment of the BWRX-300 - Step 2 Assessment of External Hazards, December 2025, ONRW-2126615823-7469.

[106] GE-Hitachi, Submission of BWRX-300 UK GDA Regulatory Query (RQ)-02127, Full Response, 1st July 2025, ONRW-2019369590-22085.

[107] NRC, www.nrc.gov/reactors/new-reactors/advanced/who-were-working-with/pre-application-activities/bwrx-300.html.

[108] ONR, Contact Record ID: ONR-NR-CR-24-335 Trilateral Regulatory Meeting on the BWRX-300 'Fault List' then 3 Successive USNRC-Led Audit Meetings on BWRX-300 Safety Strategy and PRA, August 2024, ONRW-2019369590-12814.

[109] NRC, Review of Transient and Accident Analysis Method, NUREG-0800 Chapter 15.0.2, NRC file ML070820123, March 2007.

[110] NRC, Review of Transient and Accident Analysis Method, Regulatory Guide 1.203, NRC file ML053500170, December 2005.

[111] Canadian Standards Association, Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants, N268.7-99, March 1999.

[112] NRC and CNSC, Joint Report on GE Hitachi's Containment Evaluation Method, April 2022. www.nrc.gov/docs/ml2209/ml22091A201.pdf.

[113] GE-Hitachi, Submission of BWRX-300 UK GDA - Response to RQ-02253, 8 September 2025, ONRW-609516046-2949.

[114] NRC, Regulatory Audit Report of the GE-Hitachi Nuclear Energy Americas, LLC Topic Report NEDC-33922 BWRX-300 Containment Evaluation Method, 2 March 2022, (Record ref. 2024/22621).

[115] IAEA, Safety related terms for advanced nuclear plants, IAEA-TECDOC-626, September 1991. www-pub.iaea.org/MTCD/Publications/PDF/te_626_web.pdf.

[116] ONR, Contact Record ID: ONR-NR-CR-25-097 GE-Hitachi BWRX-300 GDA - Step 2 - Instrumentation and Control International Collaboration Regulatory Presentation, 6 May 2025, ONWR-2019369590-21000.

[117] ONR, NS-TAST-GD-005 - Regulating duties to reduce risks ALARP, Revision 12, September 2024, www.onr.org.uk/operational/tech_asst_guides/index.htm.

Appendix 1 – Relevant SAPs considered during the assessment

SAP reference	SAP title
FA.4	Fault analysis: design basis analysis Fault tolerance
FA.5	Fault analysis: design basis analysis Initiating faults
FA.6	Fault analysis: design basis analysis Fault sequences
FA.7	Fault analysis: design basis analysis Consequences
FA.8	Fault analysis: design basis analysis Linking of initiating faults, fault sequences and safety measures
FA.9	Fault analysis: design basis analysis Further use of DBA
NT.1 (Target 4)	Numerical targets and legal limits Assessment against targets
AV.1	Fault analysis: assurance of validity of data and models Theoretical models
AV.2	Fault analysis: assurance of validity of data and models Calculation methods
AV.3	Fault analysis: assurance of validity of data and models Use of data
AV.5	Fault analysis: assurance of validity of data and models Documentation
AV.6	Fault analysis: assurance of validity of data models Sensitivity studies
ECS.1	Engineering principles: safety classification and standards Safety Categorisation
ECS.2	Engineering principles: safety classification and standards Safety classification of structures, systems and components
EKP.1	Engineering principles: key principles Inherent safety
EKP.2	Engineering principles: key principles

	Fault tolerance
EKP.3	Engineering principles: key principles Defence in depth
EKP.4	Engineering principles: key principles Safety function
EKP.5	Engineering principles: key principles Safety measures
SC.4	The regulatory assessment of safety cases Safety case characteristics
FA.15	Fault analysis: severe accident analysis Scope of severe accident analysis
FA.16	Fault analysis: severe accident analysis Use of severe accident analysis
FA.25	Fault analysis: severe accident analysis Relationship to DBA and PSA

Appendix 2 – Figures

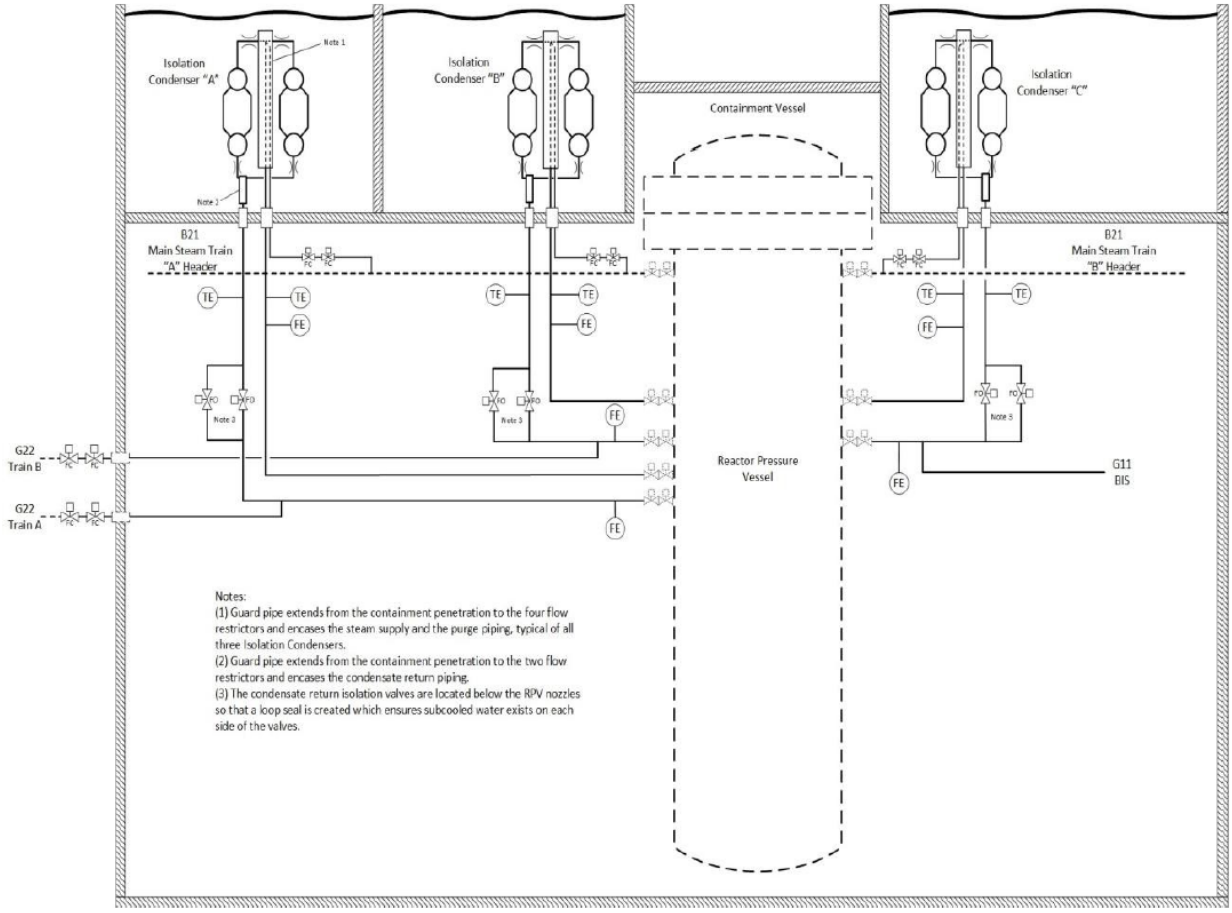

Figure 3: Isolation Condenser System Simplified Diagram[21]

[21] The RPV is taller than illustrated with a long chimney section. This promotes high natural circulation flow while providing considerable ullage space to dampen pressure transients.

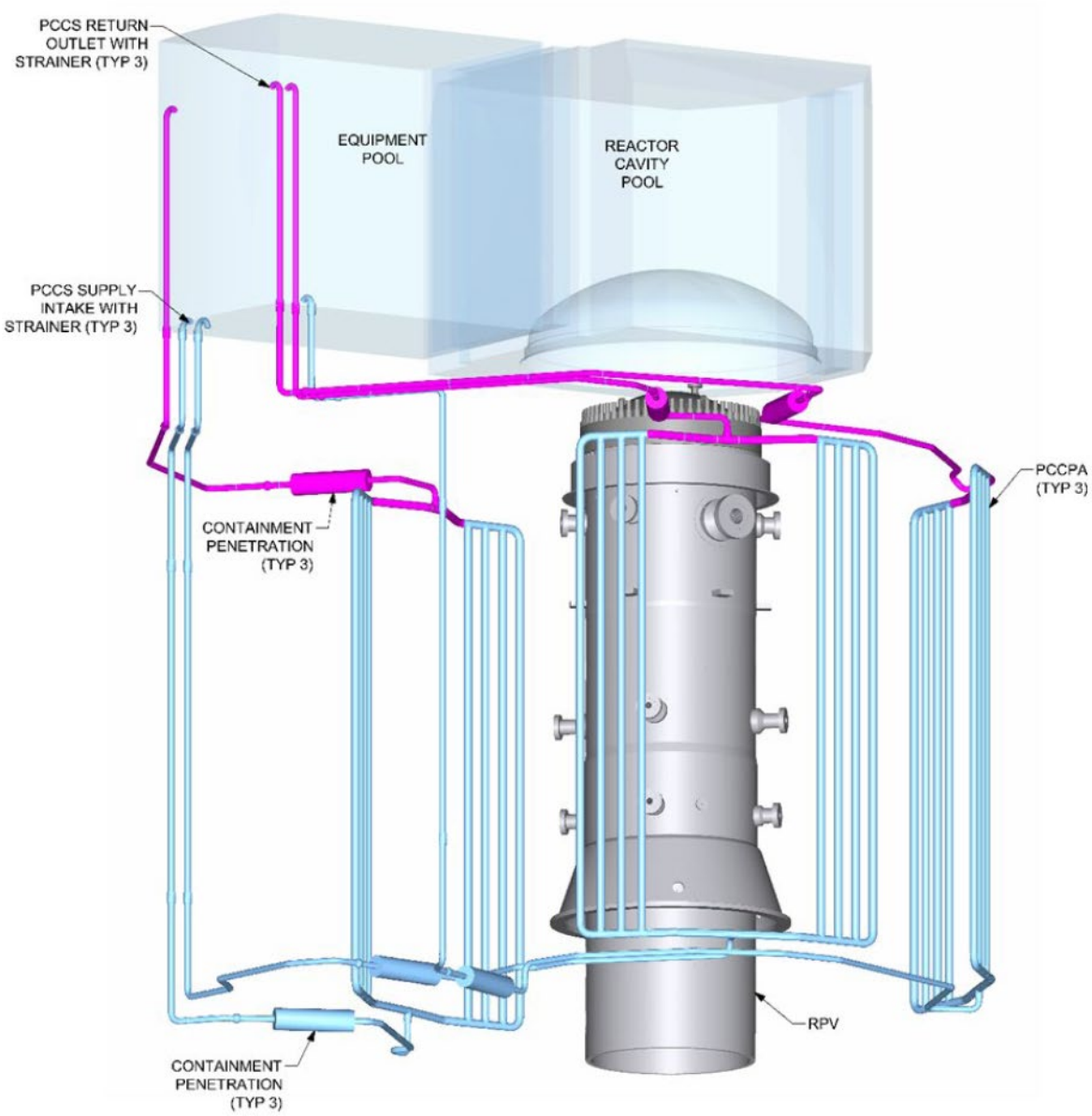

Figure 4: Passive Containment Cooling System

Appendix 3 – Findings by other regulators

This appendix provides a summary of the work undertaken by overseas regulators to review submissions in support of licensing BWRX-300 for use in the United States of America (US) and Canada. This summary focuses on their reviews of the RP's deterministic analysis of LOCAs into containment, in particular their coverage of code verification and validation matters which I take cognisance of in my assessment (see section 4.3.8).

Background

301. The US NRC have audited various Licence Topic Reports (LTRs) submitted to them by GE Vernova Hitachi Nuclear Energy Americas LLC (GVHA). Redacted versions of these LTRs (listed below) are published on the US NRCs public website (ref. [107]):

- NEDO-33910P-A, Revision 2, BWRX–300, "Reactor Pressure Vessel Isolation and Overpressure Protection."
- NEDO-33911P-A, Revision 3, BWRX–300, "Containment Performance." (which sets down the approved acceptance criteria for containment integrity)
- NEDO-33912P-A Revision 1, BWRX–300, "Reactivity Control."
- NEDC-33922P-A, Revision 3, BWRX–300, "Containment Evaluation Method (GOTHIC Application to BWRX–300)"

302. These LTRs cover various nuclear safety topics in support of future US licensing application. On completing its audits, the US NRC issue a Safety Evaluation (SE) statement which is then included in the approved LTR (denoted by 'A' appended to its identifier). The US NRC are now collaborating with CNSC on the audit of a further LTR, NEDO-33989 'Safety Strategy' with ONR also participating (Ref. [108]).

303. The similarity and common origin of the UK SSSE (specifically the PSR) to the TVA PSAR for the Clinch River site has aided collaboration with US NRC. The October 2022 OPG construction licence application for the DNNP was supported by a PSAR produced on an earlier version of the standard BWRX-300 design to that considered by ONR and US NRC. However, CNSC has been engaging continuously with OPG and GVHA as the maturing design and safety case is readied for construction..

Containment Evaluation

304. Overall, the US NRC and CNSC have reviewed and accepted the RP's "Containment Evaluation Method" addressing LOCAs into containment (covered by NEDC-33922P-A above) against the standards and guidance listed below:

- NRC, Standard Review Plan (SRP), Section 15.0.2 "*Review of Transient and Accident Analysis Methods*" (ref. [109]);
- NRC, Regulatory Guide (RG) Section 1.203 "*Transient and Accident Analysis Methods*" (ref. [110]);
- CNSC, REGDOC-2.4.1 Deterministic Safety Analysis (ref. [93]); and
- Canadian Standards Association (CSA) N286.7-99 "Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants" (ref. [111]).

305. While I have not reviewed these US NRC/CNSC documents in detail, I consider them broadly equivalent to ONR's TAGs (ref. [29]) concerning the conduct of Design Basis Assessment (NS-TAST-GD-006) and code verification/validation (NS-TAST-GD-042), and to IAEA's SSG-2 (ref. [56]) concerning deterministic safety analysis.

306. US NRC and CNSC have also jointly collaborated on a publicly available report (ref. [112]) covering the following aspects:

- Accident sequence selection
- Use of TRACG
- Selection and use of GOTHIC
- Appropriateness of PIRT
- Mixing of combustible gas
- GOTHIC nodalisation
- Uncertainties and biases
- Benchmarking against test data

307. This report concludes that these aspects are appropriate and acceptable, albeit with a need for future licensing to consider the following risks of non-condensable gas:

a) Radiolytic gas building up within the ICS (hydrogen)
b) Nitrogen ingress during small un-isolated LOCAs

308. For Step 2 GDA, the RP has provided the following evidence giving me confidence these risks can be adequately controlled in future without challenging the fundamental design:

a) Radiolytic gas (hydrogen)

After the ICS has been deployed and the standby purge line closed, this gas is expected to build up in the lower drum of the ICS heat exchanger (see Figure 3). In response to RQ-02253 (ref. [113]), the RP has provided evidence of studies which it has now undertaken to assess the impact of radiolytic gas, the measures used to control it (catalytic recombiners) and how these measures will be demonstrated in future (by analysis and validation testing).

b) Nitrogen ingress

In a small un-isolated LOCA after the ICS has deployed, it is hypothesised that RPV pressure could eventually reduce below containment pressure. Since the containment is usually filled with nitrogen, the nitrogen would then have the potential to flow into the RPV and challenge the ICS function. The RP has provided evidence of a further case study within Chapter 15.5 of the PSR (ref. [18]) indicating RPV pressure cannot fall below containment pressure leading to nitrogen ingress. By modelling suppression of the discharge at the point of pressure equalisation, this case study shows containment pressure to fall considerably faster than RPV pressure - see Figure 15.5-117 of ref. [18]. This indicates flow can only ever be out of the RPV, never inward. This case study takes no credit for the normal containment cooling system.

309. Supporting the joint US NRC/CNSC report is the detailed evidence of ref. [114]. This is the US NRC's detailed audit report of NEDC-33922P-A "Containment Evaluation Method" ((NEDC-33922P-A), which is itself supported by an independent confirmatory analysis using TRACE and MELCOR conducted by the US NRC's Office of Regulatory Research. The US NRC's Safety Evaluation statement for "Containment Evaluation Method" (NEDC-33922P-A) provides a summary of the audit's findings and the basis of the US NRC's acceptance of the following more detailed aspects:

- Mass and Energy (ME) Release (using TRACG):
    - applying the ESBWR-qualified TRACG method to BWRX-300
    - selection of pipebreak scenarios
    - channel grouping, decay heat and power shape
    - considering impact of radiolytic gas in the ICS
    - appropriateness of PIRT used for TRACG
    - suitable initial conditions and transient data
    - confirmatory sensitivity analysis using TRACE
    - adequate validation basis from previous ESBWR application

- Containment Analysis (using GOTHIC):
    - appropriateness of PIRT for a ‘dry’ containment
    - determining uncertainty and applying conservative bias (CSAU)
    - considering suitable locations/orientations of jet
    - suitability of base cases and conservative cases
    - analysis using TRACE and MELCOR
    - uncertainties and biases
    - nodalisation studies
    - adequacy of sensitivity analysis (including ‘fouling’)
    - mixing of combustible gases throughout containment sub-compartments
    - benchmarking against test data from Carolina Virginia Tube Reactor
    - Limitations and Conditions (L&Cs) concerning risks of radiolytic gas, reverse flow in the ICS and nitrogen ingress during small un-isolated LOCAs

310. Based on the audit’s review of detailed aspects, the US NRC’s Safety Evaluation statement concludes that the methods for M&E release are acceptable, based on being consistent with the US NRC’s Standard Review Plan (SRP), and are appropriately conservative, these conclusions being conditional on complying to the above Limitations and Conditions (L&Cs). The statement further concludes that the containment analysis method using GOTHIC is acceptable for demonstrating that the BWRX-300 containment design can meet the approved acceptance criteria (as set down in NEDO-33911P-A, Revision 3, BWRX–300, "Containment Performance").