Office for Nuclear Regulation

ONR Assessment Report

Generic Design Assessment of the BWRX-300 – Step 2 assessment of Control and Instrumentation

ONR Assessment Report

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

Report Title: Step 2 Assessment of Control and Instrumentation

Authored by: Control and Instrumentation Specialist Nuclear Safety Inspector, New Reactors Division, ONR

Assessment report reference: AR-01363

Project report reference: PR-01880

Report issue: 1

Published: December 2025

Document ID: ONRW-2126615823-7837

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 control and instrumentation (C&I) 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 2 of the Design Reference Report and supporting documentation. The RP uses the term instrumentation and control (I&C) throughout its documentation. C&I and I&C are equivalent terms and used interchangeably in my assessment where appropriate.

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 Great Britain, benchmarking my regulatory judgements against the expectations of ONR's Safety Assessment Principles (SAPs), Technical Assessment Guides (TAGs) and other guidance which ONR regards as relevant good practice (RGP), such as International Atomic Energy Agency (IAEA) safety, security and safeguards 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:

- high-level design principles
- reference standards and guidance
- categorisation of safety functions and classification of I&C systems
- I&C architecture and defence-in-depth
- I&C functional claims and fundamental design property claims
- plans for safety demonstration for I&C systems
- supporting essential services

- cyber security risks to safety
- ageing management

Based upon my assessment, I have concluded the following:

- The RP's design principles are sufficiently developed and demonstrate good alignment with ONR's expectations for overall design goals. Application of the design principles has resulted in a set of fundamental design properties for each I&C system, which feed into the RP's requirements management system to be substantiated at a later design stage;
- The RP's documented set of I&C reference standards and guidance provides an appropriate benchmark for RGP;
- The RP's method for categorisation and classification is, from an I&C perspective, consistent with RGP and has been applied appropriately for key I&C systems based on the design information currently available;
- The RP has identified an appropriate set of I&C systems based on the current design information, with system reliability targets within the expected ranges consistent with their safety class. The system reliability targets selected for Safety Class 2 and Safety Class 3 systems are at the more reliable end of the expected reliability claim range, and a future BWRX-300 safety case will need to provide a stronger safety demonstration for these systems reflecting these more reliable claims;
- The high-level architecture has the potential to achieve the necessary system independence. However, there are several aspects which require further development in a future BWRX-300 design and safety case including a demonstration that spurious failures of lower class systems do not result in unnecessary demands on higher class systems and that failures within the lower class systems cannot impact the delivery of safety functions of higher class systems;
- The RP has indicated that it intends to use an all-digital I&C architecture. I raised RO-BWRX300-001 as, in my opinion, the RP had down selected credible I&C platform technology options before it has demonstrated its preferred design solution can achieve the relevant safety and security expectations. In addition, the strategic decisions, design principles and supporting processes which underpin high level diversity claims are not, in my opinion, clearly identified which makes it unclear if a future safety case will be able to substantiate these claims. The RP has committed to resolving these matters within its Resolution Plan and therefore, I do not consider this to be a fundamental shortfall with the design at this stage;
- The 2-out-of-3 voting logic of the safety class 1 Primary Protection System (PPS) satisfies the single failure criterion for most plant states, except for when a maintenance bypass is applied. This does not meet the expectations of IAEA

SSG-39, which requires the single failure criterion to be met in all permissible plant states, including where part of the safety system is bypassed. The RP presented a justification within RQ-01757 which relies on the extent of diagnostic and self-test features within the PPS, the overall equipment failure rate being very low and the implementation of suitable technical specifications to limit the time at risk. A future BWRX-300 design and safety case will need to develop and substantiate the claims in this area;

- The BWRX-300 human machine interface design supports the I&C systems and the delivery of identified human actions at this stage of the design. Future design activities, such as system level failure modes and effects analyses, may result in the identification of further requirements for HMIs. The BWRX-300 has no high-integrity displays at present due to there being no identified need. A future BWRX-300 design and safety case will need to confirm that high-integrity displays and indications are not required once all human actions are identified;

- The RP has established and begun implementing an adequate framework for I&C functional and property claims;

- The RP has set out high level plans for how it intends to perform the safety demonstration of the I&C systems using the production excellence and independent confidence building measures framework. These plans are high-level and will need to be developed to support a future BWRX-300 safety case;

- Requirements and indicative high-level architecture for essential systems for I&C, namely electrical power supplies and heating, ventilation and cooling systems (HVSs), meet ONR expectations for I&C at this stage of the design. A future BWRX-300 design and safety case will need to substantiate claims which decouple HVS failures from the delivery of I&C safety functions;

- The RP has established high level interfaces between the I&C design and cyber security design processes;

- The RP has identified the need to develop plans for the management of ageing of I&C equipment and has identified RGP which supports these aims; and,

- The RP's development of its I&C systems is broadly consistent with the expectations of UK and international RGP, which provides a sound basis to reduce risks to as low as reasonably practicable.

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 and to address the remaining open actions of RO-BWRX300-001.

List of abbreviations

ABWR	Advanced Boiling Water Reactor
ALARP	As Low as Reasonably Practicable
AOO	Anticipated Operational Occurrence
APS	Anticipatory Protection System (C30)
ARI	Alternate Rod Insertion
BL	Baseline
BWR	Boiling Water Reactor
C&I	Control and Instrumentation
CAE	Claims, Arguments and Evidence
CB	Control Building
CCF	Common Cause Failure
CNSC	Canadian Nuclear Safety Commission
CRIU	Control Room Interface Unit
CS&IA	Cyber Security and Information Assurance
CSA	Canadian Standards Association
DAC	Design Acceptance Confirmation
DBA	Design Basis Accident
DEC	Design Extension Condition
DL	Defence Line
DPS	Diverse Protection System (C20)
DRR	Design Reference Report
ESBWR	Economic Simplified Boiling Water Reactor
FMCRD	Fine Motion Control Rod Drive
FW	Feedwater
GB	Great Britain
GDA	Generic Design Assessment
GVHA	GE Vernova Hitachi Nuclear Energy Americas LLC
HDL	Hardware Description Language
HMI	Human Machine Interface
HPD	Hardware Description Language Programmed Device
HVS	Heating, ventilation and cooling system
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence Building Measure
ICS	Isolation Condenser System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
L4	Level 4
LPRM	Local Power Range Monitor
MDSL	Master Document Submission List
ONR	Office for Nuclear Regulation
PA	Protected Area
PE	Production Excellence
PER	Preliminary Environmental Report
pfd	Probability of Failure on Demand

PIE	Postulated Initiating Event
PPS	Primary Protection System (C10)
PRNM	Power Range Neutron Monitor
PSAR	Preliminary Safety Analysis Report
PSR	Preliminary Safety Report
RACS	Reactor Auxiliaries Control System (C32)
RB	Reactor Building
RC&IS	Rod Control and Information System
RCS	Reactor Control System (C31)
RGP	Relevant Good Practice
RITE	Risk Informed, Targeted Engagements
RO	Regulatory Observation
RP	Requesting Party
RPV	Reactor Pressure Vessel
RQ	Regulatory Query
SAP	Safety Assessment Principle
SBWR	Simplified Boiling Water Reactor
SC	Safety Class
SC1	Safety Class 1
SC2	Safety Class 2
SC3	Safety Class 3
SCN	Non-safety class
SDD	System Design Description
SSC	Systems, Structures and Components
SSSE	Security, Safeguards and Environment Case
SyAP	Security Assessment Principle
TAG	Technical Assessment Guide
TF SCS	Regulator task force on safety critical software
TGCS	Turbine-Generator Control System
TMR	Triple Modular Redundant
TSC	Technical Support Contractor
UDH	Unit Data Highway
US	United States
US NRC	United States Nuclear Regulatory Commission
WENRA	Western European Nuclear Regulators Association

Contents

1. Introduction

1. This report presents the outcome of my control and instrumentation (C&I) 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 Chapter 7 'Instrumentation and Control' (ref. [2]) and Chapters 3, 5, 6, 8, 10, 15, 18, 25, and 27 (refs. [3], [4], [5], [6], [7], [8], [9], [10], [11]), the associated revision of the Design Reference Report (DRR) (ref. [12]) 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. [13]) and ONR's risk informed, targeted engagements (RITE) guidance (ref. [14]). The ONR Safety Assessment Principles (SAPs) (ref. [15]), together with supporting Technical Assessment Guides (TAGs) (ref. [16]), 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. [17])).

1.1. Background

4. The ONR's GDA process (ref. [18]) calls for an assessment of the Requesting Party's (RP) 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 has been supported by its supply chain partner, Amentum, who has assisted the RP in the development of the UK-specific chapters of the 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 GDA 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 is the first substantive technical assessment step, and began in December 2024 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 C&I (ref. [19]). 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. [20]) and published on the regulators' website.

14. The RP uses the term instrumentation and control (I&C) throughout its documentation. I use the RP's terminology when discussing BWRX-300 design or SSSE. C&I and I&C are equivalent terms and used interchangeably in my assessment where appropriate.

1.2. Scope

15. The assessment documented in this report is based upon the SSSE for the BWRX-300 (refs. [1], [21], [22], [3], [23], [4], [5], [2], [6], [24], [25], [7], [26], [27], [28], [29], [8], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [9], [41], [42], [43], [44], [45], [46], [10], [47], [11], [48]).

16. The RP's GDA scope has been 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. [12]) and the Master Document Submission List (MDSL) (ref. [50]). The GDA scope report 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 NPP that is proposed for consideration in the GDA. The DRR provides a list of the SSCs which are included in the scope of the GDA, and their relevant GDA reference design documents.

17. 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.

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

19. 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 ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [13]) and ONR's guidance on RITE (ref. [14]).

20. 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:

    - I&C design aspects beyond reference standards, functional and non-functional requirements and high-level architecture;
    - Details of I&C platforms beyond high-level technology; and,
    - Non-safety classified I&C systems.

21. My assessment has considered the following aspects:

    - high-level design principles
    - reference standards and guidance
    - categorisation of safety functions and classification of I&C systems
    - I&C architecture and defence-in-depth
    - I&C functional claims and fundamental design property claims
    - plans for safety demonstration for I&C systems
    - supporting essential services
    - cyber security risks to safety

- ageing management

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 SAPs (ref. [51]) 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. [52]) and nuclear security series (ref. [53]) 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. [54]), which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors (ref. [55]).

27. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the TAGs (ref. [16]). The TAGs provide the principal means for assessing I&C aspects in practice.

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

2.1.1. Safety Assessment Principles (SAPs)

29. The key SAPs applied within my assessment are:

- ECS.3 (codes and standards) – relevant to reference standards and guidance informing the BWRX-300 design;
- ECS.1 (safety categorisation) and ECS.2 (safety classification of SSCs) – relevant to the categorisation and classification of I&C systems;

- ESS.1 (provision of safety systems) and ERL.1 (form of claims) – relevant to the overall I&C architecture and system reliability targets;
- EKP.3 (defence-in-depth), EDR.2 (redundancy, diversity and segregation), EDR.3 (common cause failure), ESS.18 (failure independence), ELO.4 (layout – minimisation of the effects of incidents), and ESS.20 (avoidance of connections to other systems) – relevant to independence and reliability within the I&C architecture;
- EDR.4 (single failure criterion) – relevant to redundancy of systems within the I&C architecture;
- EKP.5 (safety measures), EHF.7 (user interfaces) and ESS.13 (confirmation to operating personnel) – relevant to displays and controls within the I&C architecture;
- ESS.2 (safety system specification) – relevant to I&C functional claims and fundamental design property claims;
- SC.2 (safety case process outputs), ESS.27 (computer based safety systems) – relevant to the safety demonstration for I&C systems;
- EES.1 (essential services – provision) – relevant to the essential services which support I&C systems; and,
- EAD.2 (lifetime margins) – relevant to ageing management planning for I&C systems.

30. A list of the SAPs used in this assessment is recorded in Appendix 1. Section 4 describes how these have been applied.

2.1.2. Technical Assessment Guides (TAGs)

31. The following TAGs have been used as part of this assessment:

- NS-TAST-GD-003 – Safety Systems (ref. [56])
- NS-TAST-GD-005 – Regulating duties to reduce risks to [as low as reasonably practicable (ALARP)] (ref. [57])
- NS-TAST-GD-046 – Computer based safety systems (ref. [58])
- NS-TAST-GD-094 – Categorisation of safety functions and classification of systems, structures and components (ref. [59])
- NS-TAST-GD-096 – Guidance on Mechanics of Assessment (ref. [13])

2.1.3. National and international standards and guidance

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

- IAEA SSR-2/1, Safety of nuclear power plants: Design, SSR-2/1 (ref. [60]);
- IAEA SSG-30, Safety classification of structures, systems and components in nuclear power plants (ref. [61]);
- IAEA SSG-39, Design of instrumentation and control systems for nuclear power plants (ref. [62]);
- IAEA SSG-61, Format and content of the safety analysis report for nuclear power plants (ref. [62]);
- IEC 61226, Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorisation of functions and classification of systems (ref. [63]);
- IEC 61513, Nuclear power plants – Instrumentation, control and electrical power systems important to safety – General requirements for systems (ref. [64]);
- IEC 60880, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions (ref. [65]);
- IEC 62138, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions (ref. [66]);
- IEC 62566, Nuclear power plants - Instrumentation and control important to safety - Development of hardware description language (HDL)-programmed integrated circuits for systems performing category A functions (ref. [67]);
- IEC 62566-2, Nuclear power plants - Instrumentation and control systems important to safety - Development of HDL-programmed integrated circuits - Part 2: HDL-programmed integrated circuits for systems performing category B or C functions, IEC 62566-2 (ref. [68]);
- IEC 60987, Nuclear power plants - Instrumentation and control important to safety - Hardware requirements (ref. [69]);
- IEC 62342, Nuclear power plants - Instrumentation and control systems important to safety - Management of ageing (ref. [70]); and,

- Regulator task force on safety critical software (TF SCS) – Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators and authorised technical support organisations (ref. [71]).

2.2. Integration with other assessment topics

33. To deliver the assessment scope described above I have worked closely with a number of 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.

34. The key interactions with other topic areas were:

- Fault studies assess requirements for I&C systems and the hazards and faults they are designed to address, including the categorisation of safety functions and classification of I&C systems, and that I&C system failures are appropriately accounted for;

- Cyber security assesses the resilience of the design to cyber security threats and vulnerabilities to ensure I&C systems operate dependably when needed. I&C supports cyber security by assessing the validity and application of necessary knowledge of the I&C safety systems for this objective;

- Electrical engineering assesses whether essential electrical services remain available for I&C safety systems. Substantiation of computer-based electrical systems, such as smart protection relays, will rely on I&C assessment;

- Mechanical engineering assesses whether dependable heating, ventilation and cooling systems (HVSs) maintain a suitable operating environment for I&C safety systems. Many of the sensors and actuators which are assessed by I&C reside within systems owned by mechanical engineering;

- Internal and external hazards assess risks to I&C operation, including potential compromises to redundancy and independence;

- Human factors engineering assess risks associated with human interaction with the plant, including with the human machine interface (HMI) of I&C systems and maintenance tasks; and,

- Fuel and Core Design assess the core monitoring system design, which is implemented in an I&C system.

2.3. Use of technical support contractors

35. During Step 2 I have not engaged Technical Support Contractors (TSCs) to support my assessment of the I&C aspects of the BWRX-300 GDA.

3. Requesting party's submission

36. 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.

37. All four volumes were subsequently consolidated to incorporate 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.

38. This section presents a summary of the RP's safety case for I&C. 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

39. The BWRX-300 is a single unit, direct-cycle, natural circulation, boiling water reactor (BWR) 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.

40. The BWRX-300 is the tenth generation of the 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.

41. 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. [6]).

42. 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. The BWRX-300 utilises natural circulation and passive cooling rather than active components, reflecting the RP's design philosophy. Many of these safety measures require I&C systems to initiate them and operate passively thereafter.

3.2. BWRX-300 case approach and structure

43. The RP has submitted information on its strategy and intentions regarding the development of the SSSE (refs. [72], [73], [74], [75]). This was submitted to ONR during Step 1.

44. 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 Great Britain (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, a Preliminary Environment Report (PER), and their supporting documents.

45. The format and structure of the PSR largely aligns with the IAEA guidance for safety cases, SSG-61 (ref. [76]), supplemented to include UK specific chapters such as Structural Integrity and Chemistry. The RP has also provided a chapter on 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). SSSE Chapter 7 ‘I&C’ is an exception and is based on a later September 2024 design reference to include key developments in the I&C architecture. 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 I&C

46. The aspects covered by the BWRX-300 safety case in the area of I&C can be grouped under 10 headings which are summarised as follows:

3.3.1. High-level principles

47. The RP has presented a set of overarching objectives and principles described within SSSE Chapter 3 ‘Safety Objectives and Design Rules for SSCs’ (ref. [3]) and within the BWRX-300 Safety Strategy (ref. [72]). The basis of the Safety Strategy is the defence-in-depth concept adopted from IAEA SSR-2/1 (ref. [60]). SSSE Chapter 3 defines a set of general design requirements applied as required throughout the design, covering codes and standards, reliability and dependability, independence, diversity, separation, single failure criterion, common cause failures (CCFs), simplicity, passive safety features and ageing management. These are applied to the I&C systems within SSSE Chapter 7 (ref. [2]).

3.3.2. Reference standards and guidance

48. The RP intends for the BWRX-300 to be an internationally harmonised design and has therefore applied internationally recognised IAEA and

International Electrotechnical Commission (IEC) standards in the design of the I&C systems. This includes IEC 61513 (ref. [64]) and its supporting standards, as well as key IAEA guidance including IAEA SSR-2/1 (ref. [60]) and IAEA SSG-39 (ref. [62]).

49. The RP has developed a Plant Instrumentation and Control Nuclear Regulations and Standards Compliance Plan (ref. [77]) which identifies three groups of standards; mandatory, reference and for information.

50. The Plan also references several relevant Institute of Electrical and Electronics Engineers (IEEE) standards and Canadian Standards Association (CSA) standards reflecting the international context of the BWRX-300 plant design.

3.3.3. Categorisation and classification of I&C systems

51. The RP's method for categorisation and classification (ref. [3]) sets out how safety functions are assigned to either safety category 1, 2, 3, or non-safety category and how SSCs are assigned to safety class (SC) SC1, SC2, SC3 or SCN in line with the requirements of IAEA SSG-30 (ref. [61]).

3.3.4. I&C architecture

52. The BWRX-300 Safety Strategy (ref. [72]) structures all SSCs within a defence in depth concept aligned with IAEA SSR-2/1 (ref. [60]). The I&C systems are allocated among defence lines (DLs), which the RP has defined as follows (ref. [72]):

- DL2 – actively control key plant parameters associated with the fundamental safety functions, and detect and mitigate anticipated operational occurrence[1] (AOO) postulated initiating events (PIEs);
- DL3 – detect and mitigate design basis accident[2] (DBA) PIEs and event sequences comprising AOO PIEs and failure of DL2 functions;
- DL4a – detect and mitigate design extension conditions[3] (DECs), including event sequences associated with some DBA PIEs and failure of DL3 functions; and,
- DL4b – detect and mitigate DECs to prevent core damage or mitigate the consequences of core damage events (severe accidents).

53. SSSE Chapter 7 (ref. [2]) describes the overall I&C architecture, as listed in Table 1 below.

[1] AOO - PIEs which occur with frequency greater than 1×10^{-2} per reactor year.

[2] DBA - PIEs which occur with frequency from 1×10^{-2} to 1×10^{-5} per reactor year.

[3] DEC - PIEs which occur with frequency less than 1×10^{-5} per reactor year.

Table 1: Systems of the BWRX-300 I&C architecture (sourced from SSSE Chapter 7 ref. [2])

Safety Class	Defence Line	System Name
SC1	DL3	C10 Primary Protection System (PPS)
SC2	DL4a	C20 Diverse Protection System (DPS)
		C22 Fine Motion Control Rod Drive (FMCRD) Motor Control System
SC3	DL2	C30 Anticipatory Protection System (APS)
		C31 Reactor Control System (RCS)
		C32 Reactor Auxiliaries Control System (RACS)
		C33 Equipment Cooling and Environmental Control System
		C34 Electrical Power Supply Control System
		C35 Reactivity Monitoring Systems
		C36 Plant Data Acquisition, Data Communications and Normal Operator Interface System
		C38 Turbine-Generator Control System (TGCS)
		C39 Normal Heatsink and Condensate/Feedwater (FW) Control System
SC3	DL4b	C37 Control and Monitoring System for DL4b Functions
SCN	N/A	C40 Investment Performance
		C41 Platform Performance Monitoring
		C43 Water Chemistry
		C44 Effluent Cleanup Control System
		C45 Network Communications and Operator Interface

54. The RP has produced a system design description (SDD) for each system. Aligned with the current degree of design maturity for the I&C systems, the SDDs for I&C systems remain under development and have not been

formally submitted to support my step 2 assessment. A selection of SDDs were provided for information.

3.3.5. I&C functional claims and fundamental design property claims

55. The RP has identified a set of fundamental safety functions, aligned with those within IAEA SSR-2/1 (ref. [60]), which are further decomposed via safety analyses. These safety functions are allocated among the I&C systems and described in SSSE Chapter 7 (ref. [2]).

56. The RP has also identified a set of general design aspects applicable to all SSCs, which are then interpreted and applied for the context of I&C systems as a set of fundamental design properties for each system. These include equipment qualification, reliability, maintenance, robustness, separation and independence, redundancy, fail safe behaviour, security, diversity and the operator interface.

3.3.6. Safety demonstration

57. The RP's SSSE case uses a formal claims arguments evidence (CAE) structure to support the safety demonstration. The BWRX-300 Safety Case Development Strategy (ref. [75]) describes the overarching CAE structure and identifies the level 3 system-level claims applicable to SSSE Chapter 7 (ref. [2]) for I&C.

58. The RP has also provided a Plant Level Instrumentation and Control Architecture Design Assurance Plan (ref. [78]) which describes how the requirements of IEC 61513 (ref. [64]) will be met.

3.3.7. Essential services

59. The RP identifies essential services supporting the delivery of safety functions by I&C systems within SSSE Chapter 7 (ref. [2]). These include the electrical power system and HVS. The BWRX-300 aims to reduce the reliance of I&C systems on essential services for the delivery of safety functions.

3.3.8. Cyber security for safety

60. Cyber security for I&C systems is discussed in SSSE Chapter 7 (ref. [2]), which references to SSSE Chapter 25 'Security' (ref. [10]). SSSE Chapter 25 (ref. [10]) details the secure by design methodology applied for the I&C systems, and the cyber security assessment process which is applied iteratively to assess cyber security risks and identify necessary controls.

3.3.9. Ageing management

61. The RP identifies general requirements for the management of ageing within SSSE Chapter 3 (ref. [3]). The Plant Level Instrumentation and Control Architecture Design Assurance Plan (ref. [78]) states that a Plant Level I&C

Maintenance Plan will be produced to satisfy the overall maintenance planning requirements of IEC 61513 (ref. [64]).

3.3.10. ALARP

62. SSSE Chapter 27 ‘ALARP Evaluation’ (ref. [11]) describes a plant wide strategy for the demonstration of ALARP. ALARP in relation to the I&C design is addressed in SSSE Chapter 7 (ref. [2]) and supported by arguments relating to RGP, operational experience, and optioneering.

3.4. Basis of assessment: RP’s documentation

63. The principal documents that have formed the basis of my I&C assessment of the SSSE are:

- SSSE Chapter 7 ‘I&C’ (ref. [2])
- SSSE Chapter 3 ‘Safety Objectives and Design Rules for SSCs’ (ref. [3])
- BWRX-300 Safety Strategy (ref. [72])
- BWRX-300 Plant I&C Systems Architecture Requirements and Design (ref. [79])
- BWRX-300 Plant Architecture Definition (ref. [80])
- BWRX-300 Plant Level Instrumentation and Control Architecture Design Assurance Plan (ref. [78])
- BWRX-300 Plant Instrumentation and Control Systems Nuclear Regulations and Standards Compliance Plan (ref. [77])
- BWRX-300 I&C Failure Mode and Hazards Analyses Plan (ref. [81])

3.5. Design maturity

64. My assessment is based on revision 3 of the DRR (ref. [12]). 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.

65. The RB and the turbine building, along with the majority of the significant 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.

66. The GDA Scope Report (ref. [49]) describes the RP’s design process that extends from baseline (BL) 0 (where functional requirements are defined) up to BL 3 (where the design is ready for construction).

67. In the March 2024 design reference, the balance of plant is at BL0 for which high-level plant requirements have been established, and SSC design remains at a high concept level.

68. SSCs in the power block are stated to be at BL1. BL1 builds on BL0 and is defined as:

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

4. ONR assessment

4.1. Assessment strategy

69. 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 I&C 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 areas to target for assessment. My assessment is consistent with the delivery strategy for the GEH BWRX-300 GDA [82].

70. GVHA is currently engaging with regulators internationally, including the Nuclear Regulatory Commission in the US (US NRC) and the Canadian Nuclear Safety Commission in Canada (CNSC); and 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.

71. Whilst there is no operating BWR plant in the UK, ONR has previously performed a four-step GDA on the Hitachi-GE UK ABWR (ref. [83]). I have taken learning from this previous assessment, 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 acceptable.

72. In line with ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [12]) and ONR's guidance on RITE (ref. [13]), I have taken a sampling approach to my assessment to inform my judgement on the adequacy of the RP's submissions. I have targeted aspects which previous ONR GDA experience shows are fundamental to I&C design, aspects which are claimed to provide significant risk reduction and aspects which I consider to be novel. I have covered all aspects identified in my assessment plan (ref. [19]), and I have refined the presentation of these within my assessment. I have sampled claims and arguments in relation to these targeted aspects.

4.2. Assessment scope

73. My assessment scope and the areas I have chosen to target for my assessment are set out in this section. This section also outlines the submissions that I have sampled, the standards and criteria that I will judge against and how I have interacted with the RP and other assessment topics.

74. 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.

75. 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 I&C. 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.

76. In order to fulfil the aims for the Step 2 assessment of the BWRX-300, I have assessed the following items, which I consider important:

- Definition, clarity and completeness of high-level principles that establish the overall design objectives for the I&C systems;
- Suitability and completeness of reference standards and guidance;
- Method for categorisation of safety functions and classification of I&C systems;
- Adequacy of the I&C architecture to ensure defence-in-depth; accounting for single failure criterion, CCF, segregation, redundancy, diversity and probabilistic reliability claims;
- Adequacy and completeness of I&C functional claims and fundamental design property claims, and their allocation to I&C systems;
- Credibility and completeness of plans for safety demonstration for I&C systems;
- Identification of and requirements for supporting essential services;
- Cyber security risks to safety; and,
- Ageing management.

4.3. Assessment

4.3.1. High-level principles

77. I reviewed the RP's high-level design principles against the benchmarks of IAEA SSR-2/1 (ref. [60]) and ONR's SAPs (ref. [15]). The RP has applied these high-level principles resulting in a set of fundamental design properties applicable to each I&C system. The design properties include performance, design for reliability, independence, qualification, verification and validation, failure modes, control of access to equipment, quality, testability and maintainability. SSSE Chapter 7 (ref. [2]) maps the fundamental design properties to sections of IEC 61513 (ref. [64]), which I consider to be RGP for I&C system design, and provides me with further confidence in the completeness of the claims. These fundamental design property requirements feed into the RP's requirements management system (ref. [84]) to be substantiated at a later design stage. My conclusion is that the I&C

design principles identified are sufficiently developed and are aligned with IAEA SSR-2/1 (ref. [60]).

4.3.2. Reference standards and guidance

78. The RP intends the BWRX-300 to be an internationally harmonised design and has applied internationally recognised IAEA and IEC standards in the design of the I&C systems. SSSE Chapter 7 (ref. [2]) states that the BWRX-300 I&C systems are designed in accordance with IEC 61513 (ref. [64]) and its supporting standards, including:

- IEC 60880 (ref. [65]) and IEC 62138 (ref. [66]) for software aspects of SC1 systems and of SC2 and SC3 systems respectively;
- IEC 62566 (ref. [67]) and IEC 62566-2 (ref. [68]) for HDL programmed device (HPD) aspects of SC1 systems and of SC2 and SC3 systems respectively; and
- IEC 60987 (ref. [69]) for hardware aspects of SC1 and SC2 systems.

79. SSSE Chapter 7 (ref. [2]) is supported by the Plant I&C Systems Nuclear Regulations and Standards Compliance Plan (ref. [77]), which describes a graded approach with three categories;

- Mandatory standards are integral to the BWRX-300 design. Any deviations are limited to special cases requiring management approval and a documented justification;
- Reference standards support mandatory standards and are generally expected to be followed. Any deviations are documented; and,
- For information standards are used to inform the design, but there is no expectation to document exactly how these have been used.

80. IEC 61513 (ref. [64]), IEC 60880 (ref. [65]), IEC 62138 (ref. [66]) and IEC 60987 (ref. [69]) are identified as mandatory standards (ref. [77]). I judge this to be appropriate as I consider these standards to be RGP for their respective areas.

81. I consider IEC 62566 (ref. [67]) and IEC 62566-2 (ref. [68]) to be RGP for HPD design. SSSE Chapter 7 did not initially refer to these standards despite being identified as reference standards in the RP's Nuclear Regulations and Standards Compliance Plan (ref. [77]).The RP confirmed within its response to RQ-01743 (ref. [85]) that HPDs are used in both SC1 and SC2 systems, which confirmed that these standards are relevant. Subsequently, the RP confirmed in its response to RQ-02005 (ref. [86]) that IEC 62566 and IEC 62566-2 are required to be applied by BWRX-300 design processes. This resulted in an update to SSSE Chapter 7 (ref. [2]), which now aligns with (ref. [77]) and refers to IEC 62566 and IEC 62566-2

for HPD design aspects. IEC 62566 and IEC 62566-2 are identified as reference standards, rather than mandatory standards in (ref. [77]). My expectation is for IEC 62566 and IEC 62566-2 to be applied for HPD design, with any deviations documented and justified. Notwithstanding this, I judge this to be appropriate on the basis of the statement of compliance in SSSE Chapter 7 (ref. [2]) and that reference standards are still expected to be followed with any deviations documented.

82. Several US (IEEE) and Canadian (CSA) standards are identified among the different categories of the RP's Nuclear Regulations and Standards Compliance Plan (ref. [77]), reflecting the international nature of the design. I consider the grouping of standards into the three categories to provide an effective mechanism for prioritisation. The BWRX-300 Design Plan (ref. [87]) explains that any conflicts in standards from different domains, if they exist, will be addressed on a case-by-case basis.

83. In conclusion, I judge that SAP ECS.3 (codes and standards) is met in principle for this stage of the design because the RP is applying RGP in the form of IEC 61513 and its supporting standards, including IEC 60880 (ref. [65]), IEC 62138 (ref. [66]), IEC 62566 (ref. [67]), IEC 65266-2 (ref. [68]), and IEC 60987 (ref. [69]).

4.3.3. Categorisation and classification of I&C systems

84. ONR's fault studies topic specialist led the assessment of the BWRX-300 categorisation and classification approach (ref. [88]) and has concluded that it is consistent with NS-TAST-GD-094 (ref. [59]) for reactor faults (ref. [89]). There is a gap in coverage for non-reactor faults which the RP has committed to resolve in a future safety case (ref. [89]).

85. I consider IEC 61226 (ref. [63]) to be RGP for categorisation and classification of I&C systems. The BWRX-300 categorisation and classification approach (ref. [88]) does not directly refer to IEC 61226. However, the approach is based on IAEA SSG-30 (ref. [61]), and IEC 61226 states that it is consistent with IAEA SSG-30. On this basis, I am content with the high level approach to categorisation and classification from an I&C perspective.

86. The BWRX-300 categorisation and classification approach (ref. [88]) has been applied to the I&C systems; for example, the PPS is SC1, DPS is SC2, and the APS, RCS, and C37 DL4b system are all SC3. I judge these classifications to be appropriate as they align with typical expectations from IEC 61226 (ref. [63]), with the principles of IAEA SSG-30 (ref. [61]), and with NS-TAST-GD-094 (ref. [59]). These systems are discussed in more detail in section 4.3.4.

87. On this basis, I conclude that the BWRX-300 categorisation and classification method (ref. [88]) as applied to the I&C systems aligns with RGP in the form of IAEA SSG-30 (ref. [61]), and satisfies SAPs ECS.1

(safety categorisation) and ECS.2 (safety classification) for this stage of the design.

4.3.4. I&C architecture

4.3.4.1. I&C systems overview

88. The BWRX-300 Safety Strategy (ref. [72]) organises all SSCs within a defence in depth concept aligned with IAEA SSR-2/1 (ref. [60]). The key I&C systems in each defence line are described in SSSE Chapter 7 (ref. [2]) and summarised as follows.

89. SC3 systems in DL2 deliver safety category 3 functions for the normal operation of the plant. For example, C31 RCS provides reactor level control, feedwater temperature control, reactor pressure control, rod control and information system and a plant automation function.

90. The SC3 C30 APS in DL2 delivers safety category 3 functions for mitigating transients in various off-normal conditions in advance of any required DL3 or DL4a response. It operates in a similar way to the PPS and DPS, by comparing signals with a setpoint and initiating safety functions when a signal is beyond the setpoint. The APS initiates hydraulic scram, performs turbine trips and manages associated turbine bypass valves (TBVs), turbine control valves (TCVs) and turbine stop valves (TSVs), RPV containment and system isolations, isolation condenser system (ICS) initiation and starts standby diesel generators. Some APS functions interface with SC1 field equipment (e.g. hydraulic scram). SSSE Chapter 7 (ref. [2]) states that there are no failures of the APS which can prevent the delivery of a higher category safety function.

91. The SC1 C10 PPS in DL3 delivers safety category 1 functions for hydraulic scram, power range neutron monitoring system (PRNM), RPV containment and system isolation, ICS initiation and ICS isolation. It receives information from dedicated plant sensors and performs signal pre-processing and logic functions to initiate its safety functions. The PPS has SC1 hardwired controls for manual initiation of safety functions and system bypass functions.

92. The SC2 C20 DPS in DL4a delivers safety category 2 functions in the case that safety category 1 functions fail to be delivered. The DPS assumes the complete failure of safety category 1 functions and is claimed to be independent and diverse from the PPS. The safety category 2 functions delivered include hydraulic scram, RPV containment and system isolations, ICS initiation, FMCRD motor run-in, and FW and condensate pump trips. The DPS also delivers the alternate rod insertion (ARI) pilot valve actuation which is a non-safety category function.

93. The SC3 C37 control and monitoring system for DL4b functions, provides the following safety functions: RPV venting control, containment venting

control, boron injection system (BIS) control and 7-day coping (indication functions).

94. The SC3 C36 Normal Operator Interface System provides the displays for the operator to view data from all I&C systems, including the PPS and DPS. The PPS also provides separate and isolated SC3 accident monitoring displays for operator monitoring for the first 72 hours after an event. The DL4b 7-day coping indication functions provide a further set of accident monitoring parameters to support the operator response after 72 hours up to 7 days.

95. In summary, the BWRX-300 I&C architecture defines a set of I&C systems within different layers of defence in depth to support the reliable initiation of key safety functions. I judge that this set of I&C systems, when combined with the fundamental design properties discussed in section 4.3.1, provides a good basis for a future safety case to demonstrate there are suitable means of initiating safety systems for the delivery of key reactor safety functions, thereby satisfying SAP ESS.1 (provision of safety systems) for this stage of the design.

4.3.4.2. Integrity targets

96. The integrity targets for each system are set out in Table 2. The system integrity targets are within the expected ranges outlined in NS-TAST-GD-003 (ref. [56]) and NS-TAST-GD-046 (ref. [58]). The claims made for the DPS and the SC3 systems are set at the more reliable end of the expected ranges. A future BWRX-300 safety case will need to provide a stronger safety demonstration for these systems than if the less reliable end of the range was claimed, to align with the expectations set out in NS-TAST-GD-046 (ref. [58]).

97. I conclude that the system integrity claims are appropriately defined and are in principle achievable, satisfying SAP ERL.1 (form of claims) for this stage of the design.

Table 2: System integrity targets (sourced from SSSE Chapter 7 ref. [2]**)**

System	C10 PPS	C20 DPS	C3x systems	C4x systems
Safety Class	SC1	SC2	SC3	SCN
Defence Line	DL3	DL4a	DL2/DL4b	N/A
Probability of failure on demand (pfd) – dangerous failures	Less than 1 x 10^{-4} pfd	Less than 1 x 10^{-3} pfd	Less than 1 x 10^{-2} pfd or less than 1 x 10^{-2} per year	N/A

98. SSSE Chapter 7 (ref. [2]) does not set out individual system-level targets for spurious actuation. However, targets for spurious actuation of key components the RP has judged to be significant to safety analyses are defined (ref. [90]). For example, a target of 1 x 10^{-2} per reactor year is set for spurious closure of TCVs or TSVs, ARI and FMCRD motor run-in functions.

99. SSSE Chapter 7 (ref. [2]) describes design features which reduce the likelihood of spurious actuation of I&C systems resulting in a safety consequence. For example, the PPS uses 2-out-of-3 voting logic to prevent spurious actuation due to single hardware failure. The PPS also fails safe such that multiple spurious hardware failures result in the delivery of the safety function. The DPS and APS have a triple modular redundant (TMR) architecture, including the use of 2-out-of-3 voting logic. The DPS and APS fail as is, such that a spurious actuation due to single hardware failures results in no spurious action. This avoids a resultant demand on the higher class PPS by a spurious failure of the lower class DPS and APS. The SC3 systems in DL2 have 3 redundancies and use voting logic to reject spurious actuations due to single hardware failures.

100. I judge the design features to prevent spurious I&C system failures provides a good basis for a future safety case to demonstrate that faults originating within a safety system are identified and protected against, in line with the expectations of SAP ESS.17 (faults originating from safety systems).

4.3.4.3. System independence

101. SAP EKP.3 outlines the principle of defence in depth, which is achieved by the provision of multiple independent barriers to fault progression. The BWRX-300 Safety Strategy (ref. [72]) sets out a plant level defence in depth concept and requires independence between DL3 and DL4a systems and DL3 and DL2 systems. This independence, ensures that at least two DLs are available to mitigate design basis events caused by single failures, and at least one DL is available against a CCF event initiated by another DL.

102. The I&C architecture aligns with the plant level defence in depth concept, with resulting claims of independence and diversity between the PPS in DL3 and the DPS in DL4a, and between the PPS in DL3 and SC3 systems in DL2. These claims of independence are essential for the reliable initiation of safety functions. The remainder of this subsection discusses plant level aspects relevant to the independence of I&C safety functions. Subsections 4.3.4.4 to 4.3.4.8 address further aspects of independence, addressing platforms, sensors, actuators, communications, separation, and segregation. I summarise my judgements in relation to independence in the I&C architecture in subsection 4.3.4.9.

103. The plant level defence in depth concept has been considered at a plant level by ONR's fault studies inspector (ref. [89]) resulting in the identification

of the following potential shortfalls relating to independence in overall end-to-end safety functions, which provide relevant context to my assessment of independence of I&C systems:

- DL2, DL3 and DL4a rely on the insertion of control rods to achieve reactor shutdown. There is an overall limit to the reliability that can be claimed for reactor shutdown by the hydraulic or motor-driven insertion of control rods, as described in the RP's response to RQ-01875 (ref. [91]). The BWRX-300 has an alternative means of shutdown, the BIS, within DL4b. However, it is currently not claimed in the deterministic safety analysis. A commitment is made under forward action plan item 15.5-29 (ref. [92]) to demonstrate diversity in the designated protection for all frequent faults and to confirm the status of the BIS.

- DL2, DL3 and DL4a rely on the ICS to deliver heat removal safety functions. ONR's fault studies inspector has identified various features which lend credibility to a high reliability claim and identified various aspects of future work. This leads to an overall judgement that the high reliability claim on the ICS is practicable at GDA Step 2 (ref. [89]).

104. A result of the plant level defence in depth concept is that DL2 and DL4a are not claimed to be independent. Full or partial failures of systems in DL2 can result in initiating events. The response to these events can only rely on systems in DL3, because the systems in DL4a may also be affected by the same initiating failure as they are not fully independent of DL2. SSSE Chapter 15.5 'Deterministic Safety Analysis' (ref [34]) addresses such cases and shows an appropriate DL3 response meeting acceptance criteria.

105. In addition, an initiating event arising from a full or partial failure of a DL2 system combined with a failure of DL3 systems to respond has an overall sequence frequency of 1×10^{-6} per reactor year, which falls within the design basis expectations of SAP FA.6 (Fault sequences) and therefore expected to be addressed in the deterministic safety analysis. Such events are not currently assessed. A future BWRX-300 safety case will need to demonstrate an appropriate response to such events. The RP confirmed in its response to RQ-02425 (ref. [93]) that such events are not addressed within the analyses supporting the standard BWRX-300 design, but will be addressed by future UK-specific safety case development under forward action plan item 15.5-30 (ref. [92]). I do not consider this a fundamental shortfall at GDA Step 2 because of the commitments made to address this in a future safety case. Other design and safety case developments may also be relevant to this demonstration, such as clarification of the role of the BIS (per forward action plan item 15.5-29 (ref. [92])) and the technologies deployed in the I&C architecture (see RO-BWRX300-001 (ref. [94]) discussion in Section 4.3.4.4).

106. I raised a specific example of this type of event which was prominent during the UK ABWR GDA, where it was identified that a failure of the digital Rod

Control and Information System (RC&IS) could result in the concurrent insertion of all control rods at a slow speed causing fuel failure (ref. [95]). The RP confirmed it was aware of this experience from UK ABWR, but the analysis to identify these types of failures for BWRX-300 had not yet been performed (ref. [96]). The RP confirmed it will be addressed in a future BWRX-300 safety case by the analysis of partial and total system failures to complete the fault list, as part of forward action plan item 15.5-30 (ref. [92]), which I judge to be appropriate at GDA Step 2.

107. The RP has not significantly progressed the design of the severe accident I&C equipment in DL4b at GDA Step 2. However, the RP has set out the principle that equipment performing DL4b functions are independent of any equipment which may have failed in the event sequence those functions are mitigating, which I judge to be appropriate for GDA Step 2 and aligned with SAP EKP.3 (defence in depth).

4.3.4.4. System independence - platforms

108. Independence between I&C systems can be undermined by latent systematic errors, which if triggered at the same time, can result in the CCF of otherwise independent I&C systems. High-quality development processes and simplicity are important principles for the reduction in the number of systematic errors in the first place. Diversity is then a complementary method which introduces deliberate differences between I&C systems to reduce the likelihood that any residual systematic errors are common and triggered at the same time.

109. SSSE Chapter 7 (ref. [2]) states that digital platforms are used for the PPS, DPS and SC3 systems in DL2. The RP initially considered using analogue technology for the DPS (ref. [12]). However, as the BWRX-300 I&C continued to develop, the DPS concept design evolved to use a digital platform.

110. IAEA SSG-39 (ref. [62]) identifies several different types of diversity. One of which is equipment diversity, which is achieved by using equipment that employs different technology. I raised RQ-01756 to understand the reasons why the RP had decided to adopt digital technology over hardwired technology for the DPS as, in my opinion, it appeared to reduce the degree of equipment diversity in the I&C architecture. The RP's response to RQ-01756 (ref. [97]) identified several constraints of analogue technology, such as physical space, power consumption, and heat loading, which led the RP to conclude that digital technology was preferable.

111. Equipment diversity can also be achieved using different types of digital technology, such as using computer based equipment versus HPDs (ref. [62]). I raised RQ-01743 to understand the types of digital technology proposed for use in the PPS and DPS. The RP's response to RQ-01743 (ref. [85]) states that the PPS and DPS are implemented using a mixture of different digital technologies, with both systems using both HPDs and

microprocessors. In my opinion, this selection of technology appears to have limited equipment diversity.

112. IAEA SSG-39 (ref. [62]) and IEC 61513 (ref. [64]) require a demonstration that the types of diversity chosen achieve the common cause mitigation that is claimed. A complete demonstration is not expected at GDA Step 2 given the extent of design maturity. However, given the RP's choice of technologies in the I&C architecture, I was seeking confidence that the design could support a future safety case to successfully make this demonstration.

113. I raised RQ-01961 to further understand the RP's approach to diversity demonstration. The RP's response to RQ-01961 (ref. [98]) describes how it had not been possible to perform an assessment of potential CCFs to inform the DPS technology selection, as it required a preliminary design of the DPS to be available. Instead the RP stated that NUREG/CR-6303 (ref. [99]) and NUREG/CR-7007 (ref. [100]) were used to inform design decisions. Once a preliminary DPS design using digital technology was available, the RP performed a preliminary diversity assessment (ref. [101]) using the semi-quantitative methodology provided in NUREG/CR-7007 to provide confidence that sufficient diversity could be demonstrated. This assessment will be updated in a final diversity assessment at a later design stage. In my opinion, NUREG/CR-6303 and NUREG/CR-7007 provide a useful framework to consider the factors contributing to I&C diversity, and are RGP in this regard. However, NUREG/CR-7007 also provides a semi-quantitative assessment methodology which may provide insights for design refinement, but I do not consider it to be a suitable demonstration of diversity by itself. My opinion is aligned with US NRC BTP 7-19 (ref. [102]), which states "this method has not been benchmarked and should not be used as the sole basis for justifying adequate diversity." My expectation is that potential CCFs should be systematically identified, and specific design decisions and features should be incorporated which eliminate these where possible, or provide adequate mitigation.

114. While the RP has made high-level claims of diversity between defence lines, the strategic decisions, design principles and supporting processes which underpin these diversity claims are not, in my opinion, clearly identified which makes it unclear if a future demonstration could be successful. It is therefore not possible to confirm, at this stage, if the design will support claims of independence between lines of defence in depth as required by SAP EKP.3 (defence in depth) and IAEA SSR-2/1 (ref. [60]) Requirement 7.

115. As a result of my enquiries and engagements with the RP, and my sample related to equipment diversity, I raised RO-BWRX300-001 (ref. [94]) as, in my opinion, the RP has down selected credible options before it has demonstrated its preferred design solution can achieve the relevant safety and security expectations.

116. I raised four actions within RO-BWRX300-001 (ref. [94]):

- Action A1 – Provide a delivery plan – Provide a delivery plan, supporting the RO Resolution Plan, which provides further details as to how the RP intends to satisfy the objectives of each RO action;
- Action A2 – Diversity attributes supporting independence claims within the I&C architecture – Capture in an appropriate report how the BWRX-300 I&C architecture incorporates specific diversity attributes, resulting in identifiable design decisions and features, which allow a credible demonstration to be made that the nuclear safety risks arising from CCF as a result of loss of independence between I&C systems have been reduced, so far as is reasonably practicable. This report should show how these attributes, decisions and features will be supported by claims and arguments in a future safety case;
- Action A3 – Cybersecurity supporting independence within the I&C architecture – Capture in an appropriate report the activities and assessments which will result in identifiable design decisions and features which support a credible demonstration to be made that the nuclear safety risks arising from common cyber security vulnerabilities undermining independence between I&C systems have been adequately mitigated; and,
- Action A4 – Justification of I&C technology selection – Capture in an appropriate report a suitable and sufficient justification for the technology type(s) selected for the I&C systems within the BWRX-300 I&C architecture with a view that this will support claims and arguments in a future safety and security case.

117. The RP has produced a Resolution Plan (ref. [103]) describing how each RO action is to be met. In addition, as required by Action 1 of RO-BWRX300-001, the RP has produced a Delivery Plan (ref. [104]) setting out further detail as to how each of the other RO actions will be addressed. The remaining actions will be completed beyond GDA Step 2.

118. The Resolution Plan (ref. [103]) and Delivery Plan (ref. [104]) outline activities which, in my opinion, will guide and inform the development of the BWRX-300 I&C architecture and systems design, and support the production of a robust future safety case in this area. The Delivery Plan (ref. [104]) indicates that these activities are being integrated within the BWRX-300 standard plant design process, with the exception of some UK specific cyber security activities within Action 3. The activities outlined in Action A2 and A3 address the guiding principles of diversity and security by design to support a holistic approach to design. The activities culminate in Action A4 where the RP will assess the available technology options and justify the selection of the technology selected in the I&C architecture. In my opinion,

these activities will support the RP to continue to develop the I&C design and safety case in a way which aligns with overall design goals.

119. In summary, while SSSE Chapter 7 (ref. [2]) does not, in my opinion, fully meet the expectations set out in SAP EKP.3 (defence in depth), IAEA SSR-2/1 (ref. [60]) Requirement 7, and NS-TAST-GD-046 (ref. [58]), the RP has committed to resolving this within its Resolution Plan (ref. [103]) and therefore, I do not consider this to be a fundamental shortfall with the design at this stage.

4.3.4.5. System independence - sensors

120. The arrangement of sensors is informed by the plant level defence in depth concept, as discussed in Section 4.3.4.3. A set of SC1 sensors and associated interfacing equipment provide inputs to the PPS in DL3. Each division of PPS is connected to dedicated sensors separate from the other two divisions. A set of SC2 sensors and interfacing equipment provide inputs to the DPS in DL4a, and in some cases to SC3 systems in DL2. The plant level defence in depth concept claims independence between DL3 and DL4a, and DL3 and DL2. The sensors supporting the PPS are therefore claimed to be independent and diverse of those supporting the DPS and SC3 systems in DL2, which I judge to align with the principles of SAP EKP.3 (defence in depth), subject to the wider consideration of the plant level defence in depth concept as discussed in Section 4.3.4.3. At GDA Step 2, the initiating signals for different safety functions are identified, but no further details are available regarding the sensors to underpin the claims of independence and diversity. I consider this to be appropriate at GDA Step 2, but note that a future safety case will need to demonstrate independence and diversity between SC1 and SC2 sensors.

121. The RP has not made a claim of independence and diversity between DL2 and DL4a. I discuss this approach in Section 4.3.4.3. Notwithstanding this, a result of this approach is that the DPS in DL4a and SC3 systems in DL2 are permitted to share sensors. In such cases, the sensors are classified SC2 in line with the highest safety function that they deliver, and SC2 signal splitters are used to prevent the propagation of electrical faults from lower class to higher class systems. I judge the use of SC2 signal splitters to provide a suitable means of preventing failures propagating from lower to higher class systems, thereby satisfying an expectation of IEC 61513 (ref. [64]) and the guidance accompanying SAP ECS.2 (safety classification of SSCs). In some cases, the RP has provided an additional SC3 sensor to support continued operations should there be a failure of the SC2 signal splitters.

4.3.4.6. System independence - actuators

122. The interface between I&C systems and mechanical equipment is informed by the plant level defence in depth concept, discussed in Section 4.3.4.3, which requires independence between DL2 and DL3, and DL3 and DL4a. Section 4.3.4.3 identifies areas where further work is required which may

affect the interface between I&C systems and mechanical equipment, such as the provision of alternate means of reactor shutdown and the reliability of the ICS. Notwithstanding these, a result of the plant defence in depth strategy is that the PPS in DL3 has independent actuators from the DPS in DL4a and SC3 systems in DL2.

123. The PPS, DPS and APS are able to actuate the same mechanical equipment. The suitability of the sharing of the mechanical equipment is addressed at a plant level and discussed in Section 4.3.4.3. Notwithstanding this, I judge that the proposed actuator arrangement is suitable because each I&C system is able to independently initiate the safety feature and the arrangement ensures that a lower class system cannot prevent the delivery of a safety function by a higher class system, thereby satisfying the guidance accompanying SAP ECS.2 (safety classification of SSCs).

124. While this actuator arrangement supports independence between systems of different safety classification, the arrangement has the potential for spurious actuation caused by lower class systems. As discussed in section 4.3.4.2, the SC2 DPS and SC3 APS include features intended to reduce the frequency of unnecessary hydraulic scrams and consequent demands on the SC1 PPS, such as TMR architectures including 2-out-of-3 voting logic and use self-diagnostic and self-test functions which fail as is upon a detected failure and alert the operator.

125. I judge that the interface between the I&C architecture and the actuators is aligned with SAP EKP.3 (defence in depth). SSSE Chapter 7 (ref. [2]) identifies various features of the DPS and APS which, in my opinion, should support a future demonstration that spurious failures of lower class systems do not result in unnecessary demands on higher class systems. This will need to be demonstrated in a future BWRX-300 safety case to align with guidance in NS-TAST-GD-046 (ref. [58]). However, I consider this to be routine design and safety case development and do not consider it a fundamental shortfall for the purposes of my GDA Step 2 assessment.

4.3.4.7. System independence - communications

126. The I&C architecture includes features to ensure that communications between I&C systems do not undermine independence. Generally, communication links between systems of different safety classification are avoided. Where unavoidable, the RP has used one-way isolation devices to ensure that failures cannot propagate from a lower-class system to a higher-class system. The safety class of the isolation device is the same as the higher-class system. I judge the use of such isolation devices to be appropriate because it aligns with SAP ESS.20 (avoidance of connections to other systems) and the guidance accompanying SAP ECS.2 (safety classification of SSCs).

127. An exception to communications independence I have identified during GDA Step 2 is to facilitate periodic gain factor adjustment of PPS Local Power

Range Monitors (LPRMs). This adjustment is typical for BWRs and needed to account for detector depletion during operation. Gain adjustment factors are calculated by the SC3 C35 Reactivity Monitoring System and must be transferred to the SC1 PPS. The BWRX-300 has a semi-automated means to transfer the gain adjustment factors, with the intent of reducing the likelihood of human error and operator burden.

128. I raised RQ-01937 for the RP to explain how a foreseeable error or maloperation of this semi-automated data transfer could not prevent the correct and timely operation of safety functions. The RP's response to RQ-01937 (ref. [105]) explains that the gain adjustment factors are transferred from C35 to a Control Room Interface Unit (CRIU), which is a SC3 part of the PPS. The CRIU provides a means to prevent the propagation of errors from a lower class to higher class system by allowing the operator to review and positively confirm the gain factors from C35, controlling the communications interface between C35, the CRIU and the PPS logic module, and reading back the data from the PPS logic module for operator confirmation. The CRIU can only communicate with one system at a time, either C35 or the PPS logic module.

129. The semi-automated transfer of LPRM gain factors remains subject to further design development. Through my engagements with the RP, I have gained confidence that the RP understands the principles of communications independence. Notwithstanding this, a future BWRX-300 safety case will need to demonstrate how the parameters are set correctly with the necessary high confidence to support delivery of safety category 1 safety functions, and demonstrate how the design prevents failures of a lower class system affecting the delivery of safety functions by a higher class system to satisfy the guidance supporting SAP ECS.2 (safety classification of SSCs).

130. A further exception to communications independence I have identified is to support rod position control, control rod block signals and withdrawal sequencing. Commands for these safety category 3 functions are sent from the SC3 C31 RC&IS to the SC2 C22 FMCRD motor controllers system via a network link. The SC2 C22 FMCRD motor controllers system also receives signals from the SC2 DPS for safety category 2 functions such as control rod run-in. These safety category 2 commands are sent via a hardwired connection separate to the network link used for safety category 3 commands. The SC2 FMCRD Motor Controllers include priority logic to ensure that safety category 2 functions are prioritised over safety category 3 functions.

131. My engagements with the RP during GDA Step 2 has given me confidence that the RP understands the principles of communications independence and is continuing to develop and optimise the design to be robust against potential CCFs, especially where there are exceptions to independence principles. A future BWRX-300 safety case will need to demonstrate how the design prevents faults or failures within the lower-class systems from

impacting the delivery of safety functions of higher-class systems to satisfy the guidance supporting SAP ECS.2 (safety classification of SSCs).

4.3.4.8. System independence - separation and segregation

132. Physical separation, barriers and civil structures will be needed to achieve necessary independence, particularly against internal hazards. The assessment of independence in the presence of foreseeable internal hazards is carried out by ONR's internal hazards inspector (ref. [106]), and has concluded that the RP has considered the fundamental aspects of segregation and separation in the overall layout design at GDA Step 2, in line with SAP ELO.4 (layout).

133. The RP has identified requirements to ensure sufficient resilience of the I&C systems to foreseeable hazards. For example, SC1 PPS equipment is located in three separate divisional fire barrier rooms in the RB. The RB rooms are seismically qualified and environmentally controlled. The I&C equipment is qualified in accordance with relevant IEC nuclear standards; IEC/IEEE 60780-323 Qualification (ref. [107]) and IEC/IEEE 60980-344 Seismic Qualification (ref. [108]). I judge that the fundamental principles identified by the RP meet the segregation expectations of SAP EDR.2 (redundancy, diversity and segregation) and are likely to support a demonstration of adequate segregation and separation of I&C systems in a future safety case.

4.3.4.9. System independence - summary

134. In summary, the high-level I&C system architecture forms a good basis to meet SAPs EKP.3 (defence in depth), EDR.2 (redundancy, diversity and segregation), EDR.3 (common cause failure) and ESS.18 (failure independence). I also consider that the I&C architecture aligns with the defence in depth requirements set out in IAEA SSR-2/1 (ref. [60]).

135. I have identified a perceived gap in relation to demonstration of independence between the PPS and DPS/SC3 systems given the all-digital architecture proposed at GDA step 2. As a result, I raised RO-BWRX300-001 (ref. [94]). However, I consider there to be a route forward supported by the activities set out in the RP's Resolution Plan for RO-BWRX300-001 (ref. [103]). In my opinion, if this resolution plan is followed and it successfully develops the design and substantiates safety case claims, this should not be a barrier to a future safety case demonstrating why the BWRX-300 can be built in GB.

136. Based on my sample, in two areas, a future BWRX-300 design and safety case would need to demonstrate:

- That the various features of the DPS and APS ensure spurious failures of lower class systems do not result in unnecessary demands on higher class systems, aligned with NS-TAST-GD-046 (ref. [58]); and,

- That failures within the lower-class systems cannot impact the delivery of safety functions of higher-class systems to satisfy the guidance supporting SAP ECS.2 (safety classification of SSCs) and address the cybersecurity aspects of any such arrangements.

It is my opinion that these aspects can be resolved during future design development to support a future safety case and should not be considered a fundamental shortfall in the design.

4.3.4.10. Redundancy and single failure criterion

137. The I&C system redundancies are presented in Table 3. This has been driven by reliability requirements, and the single failure criterion where applicable.

Table 3: I&C system redundancies (sourced from SSSE Chapter 7 ref. [2])

I&C system	Safety Class	Redundancy
PPS	SC1	3
DPS	SC2	3
APS	SC3	3
RCS	SC3	3
C3x Systems	SC3	3 (generally)
C4x Systems	SCN	N/A

138. The SC1 PPS has 3 redundancies to satisfy the single failure criterion, accounting for the consequential loss of one redundancy from an initiating event. The PPS uses 2-out-of-3 voting logic. The PPS applies fail safe principles such that when a diagnostic failure is revealed, the corresponding division provides a vote for the safe state.

139. The PPS allows the operator to place a single division in maintenance bypass. The bypass control is a mechanical switch that can only be placed in position to bypass one division of PPS at a time. When the maintenance bypass is applied, the bypassed channel is ignored from the voting logic to become 2-out-of-2.

140. SAP EDR.4 (single failure criterion) states that during any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. IAEA SSG-39 (ref. [62]) 6.13 further elaborates that “each safety group should perform all actions required to respond to a postulated initiating event in the presence of

any single detectable failure within the safety system, in combination with: any undetectable failures [… and] the removal from service or the bypassing of part of the safety system for testing or maintenance that is allowed by plant operating limits and conditions". Therefore, in my opinion, the PPS does not meet the single failure criterion when a maintenance bypass is applied.

141. I raised this with the RP, and the RP has stated in response to RQ-01757 (ref. [109]) that there is no scheduled or planned online testing of the PPS due to the use of extensive diagnostic and self-test features. The RP states that the maintenance bypass is only used for limited time periods to resolve equipment failures, which are expected to be infrequent due to the high reliability of the PPS equipment and are governed by administrative controls. The RP states that this arrangement aligns with IEEE 603 (ref. [110]) clause 6.7. The RP also notes the availability of the DPS as a backstop to ensure overall plant safety goals are satisfied.

142. A future BWRX-300 design and safety case will need to demonstrate that risks associated with maintenance states of the PPS are adequately managed. I expect this to establish and substantiate claims regarding equipment failure rates and the extent and effectiveness of diagnostic and self-test features of the PPS, with appropriately defined technical specifications to limit the time and conditions within which such a bypass can be applied to justify that SAP EDR.4 (single failure criterion) and fault detection guidance within NS-TAST-GD-046 (ref. [58]) are met. Should these claims not be substantiated in the future, then it may be necessary for the RP to increase the redundancy of the PPS to meet the expectations of the single failure criterion in maintenance states, as defined in IAEA SSG-39 (ref. [62]).

143. The redundancy provided for other systems is provided for system reliability purposes. The expectation of IEC 61513 (ref. [64]) and SAP EDR.4 (single failure criterion) is for the single failure criterion to be met for category A safety functions (i.e., Safety Category 1 functions in the BWRX-300 categorisation and classification scheme), and it is therefore not a requirement for I&C systems other than the PPS to comply with the single failure criterion.

4.3.4.11. Displays and controls

144. The BWRX-300 has two key HMIs. The primary locus of control and monitoring is the main control room (MCR) situated within the CB. If the MCR becomes uninhabitable, or control and monitoring becomes untenable due to MCR HMI failures, a Secondary Control Room (SCR) is provided within the RB. The MCR and SCR contain the controls and displays necessary to allow operators to monitor the plant and deliver any necessary safety functions.

145. The BWRX-300 Safety Strategy (ref. [72]) states a design aim to reduce the reliance on human actions following an event. The BWRX-300 is designed such that the fundamental safety functions are delivered for any event sequence in the AOO or DBA event categories for 72 hours with no operator action.

146. The primary means of monitoring the plant from both the MCR and SCR is via an SC3 screen-based HMI. The data from the SC1 PPS, SC2 DPS and SC3 systems are provided to the unit data highway (UDH) network within the C36 system. The C36 system includes the necessary displays, controls and alarm systems to support operator actions, using the data from the UDH. The PPS and DPS connections are via one-way isolation devices of commensurate safety class to avoid the propagation of failures from lower to higher class systems. Manual hardwired controls of corresponding safety class are provided for the manual initiation of safety features and for operator actions such as system reset, maintenance bypass and calibration.

147. The PPS also has a dedicated set of SC3 accident monitoring displays. These provide a limited set of parameters to support the operator to monitor a plant event and confirm the performance of the necessary safety functions. It is intended to be used for the first 72 hours after an event. The accident monitoring displays are directly connected to the PPS via a one-way connection, and do not connect to the UDH or to the other displays within the C36 system.

148. The SC3 C37 DL4b system delivers the 7-day coping indication functionality for severe accident management. There is limited information on this system available in SSSE Chapter 7 (ref. [2]). Through my engagements with the RP (ref. [111]), I confirmed that this aspect of the design remains under development and it was not yet confirmed whether the C37 system would require dedicated indications or if it would be integrated with indications from other systems. However, the key principle is established in SSSE Chapter 7 (ref. [2]) that, “equipment performing DL4b safety functions are independent of any equipment postulated to have failed in the event sequence those functions are mitigating.” I judge this to be appropriate for GDA Step 2 because it aligns with SAP ESS.3 (monitoring of plant safety) and the requirements of IAEA SSG-39 (ref. [62]) 8.27 that accident monitoring functions “should not be disabled by the operation, failure or mal-operation of I&C equipment that is not part of the severe accident monitoring instrumentation.”

149. The design of the HMIs fulfil the design requirements identified at this stage of the BWRX-300 design. Future design activities, such as system level failure modes and effects analyses (ref. [81]), may result in the identification of further requirements for HMIs. While no safety category 1 operator actions have been identified at this design stage, the RP has stated that any operator actions necessary to deliver safety functions in a design basis event would be Safety Category 1 safety functions (ref. [88]).

150. I judge that the overall architecture of displays and controls are suitable to support the safety functions identified at this stage of the design. However, I consider the absence of high integrity indications to be novel to the UK. High integrity indications of key plant parameters are usually claimed to support the operator to positively confirm that the safety systems have initiated and achieved their safety functions, and to maintain situational awareness of the state of the plant in an event, aligned with SAP ESS.13 (confirmation to operating personnel) and EHF.7 (user interfaces). Such indications also support the operator to maintain the safety systems by providing the interface for applying operational bypasses for testing and calibration.

151. While the objective to reduce reliance on human actions is well aligned with the engineering hierarchy of controls set out in SAP EKP.5 (safety measures), a future BWRX-300 safety case will need to justify the classification of displays once all human actions are identified in response to events and to maintain the safety systems. Relevant cyber security aspects, such as the principle of secure by design, would also need to be addressed. It is my opinion that the RP should be able to develop an adequate future safety case, and that the RP would be able to include appropriate indications in the design if a future analysis identified a need for high integrity indications. I therefore, do not consider this to be a fundamental shortfall.

4.3.5. I&C functional claims and fundamental design property claims

152. The RP has identified a set of fundamental safety functions, aligned with those within IAEA SSR-2/1 (ref. [60]). The BWRX-300 Safety Strategy (ref. [72]) describes how these fundamental safety functions are developed and elaborated through the safety evaluation and analysis framework resulting in a set of system level safety functions. The safety functions are listed within a fault list and allocated among the I&C systems as described in SSSE Chapter 7 (ref. [2]).

153. The RP has also identified a set of general design aspects applicable to all SSCs, which are then interpreted and applied for the context of I&C systems as a set of fundamental design properties for each system as presented in SSSE Chapter 7 (ref. [2]). These general design aspects include equipment qualification, reliability, maintenance, robustness, separation and independence, redundancy, fail safe behaviour, security, diversity and the operator interface.

154. I&C system functional claims and fundamental design property claims are expressed as system level requirements. These are developed and elaborated according to the RP's I&C Architecture Design Assurance Plan [78], and supported by the RP's Requirements Management Plan (ref. [84]).

155. From the submissions at GDA Step 2, I judge that the RP has established and begun implementing an adequate framework to satisfy SAP ESS.2 (safety system specification). It is not possible or expected at GDA Step 2 to demonstrate completeness of I&C system functional claims and fundamental

design property claims but based upon my sample I judge that a future BWRX-300 safety case could make this demonstration.

4.3.6. Safety demonstration

4.3.6.1. Overall framework

156. The RP has structured the SSSE Case using a CAE approach centred on the fundamental objective that:

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

157. This fundamental objective is broken down into claims structured in 3 levels. The BWRX-300 Safety Case Development Strategy (ref. [75]) describes the overarching CAE structure and identifies the level 3 system-level claims applicable to SSSE Chapter 7 for I&C. SSSE Chapter 7 contains a CAE route map appendix, which identifies the applicable level 3 claims and where the associated sub-claims and arguments are located in the main body of the document. The RP has not adopted a formal referencing system for sub-claims and arguments, which are presented in a narrative form, using requirements as a proxy for sub-claims. The narrative form used addresses the aspects identified within IAEA SSG-61 (ref. [76]) as appropriate for the current level of design maturity. These requirements are managed according to the RP's Requirements Management Plan (ref. [84]) for future substantiation.

158. In summary, from an I&C perspective, I judge that SSSE Chapter 7 is aligned with the guidance in IAEA SSG-61 (ref. [76]) with detail proportionate to the stage of design. I judge that the framework established in SSSE Chapter 7 provides a means for the RP to satisfy SAP SC.2 (safety case outputs) in the future.

4.3.6.2. I&C safety demonstration planning

159. The RP has produced a Plant Level Instrumentation and Control Architecture Design Assurance Plan (ref. [78]) which sets out the I&C design process, the outputs which will be produced, and how the process satisfies the requirements of IEC 61513 (ref. [64]). The RP intends this document and its future implementation to support the demonstration of production excellence (PE) for the I&C systems.

160. The RP has identified in SSSE Chapter 7 (ref. [2]) the need to implement independent confidence building measures (ICBMs) and provided examples of techniques and measures applicable to each safety class of equipment in a graded approach. The techniques and measures align with ONR's guidance to its inspectors set out in NS-TAST-GD-046 (ref. [58]).

161. I consider the high level approach outlined by the RP in relation to PE and ICBMs are aligned with SAP ESS.27 (computer-based safety systems) and NS-TAST-GD-046 (ref. [58]), and the RP has demonstrated awareness of these expectations. However, a future BWRX-300 safety case will need to further establish and implement these plans.

4.3.6.3. Smart devices safety demonstration planning

162. SSSE Chapter 7 (ref. [2]) states that smart devices are only used in SC3 and SCN applications. The RP has not yet developed its plans for the safety demonstration of smart devices. However, given the constraint that SSSE Chapter 7 (ref. [2]) defines which limits use of smart devices to SC3 and SCN applications, I am confident that development of a suitable methodology to qualify smart devices for such applications will be possible. I note that the RP has identified IEC 62671 (ref. [112]) in the Nuclear Regulations and Standards Compliance Plan (ref. [77]), which is a relevant standard in this area.

163. There are applications for which it is becoming increasingly difficult to procure non-smart devices. A common example is electrical protection relays. In collaboration with ONR's electrical engineering inspector (ref. [113]), the RP's response to RQ-01844 on electrical protection relays reaffirmed this limitation on use of smart devices to SC3 and SCN (ref. [114]). However, I note that other duty holders in the UK have qualified smart devices to higher safety classifications, although the success of this requires early identification of the need and development of a robust qualification process and plan.

164. Despite the limited information available at GDA Step 2, I am confident that it will be possible to develop a suitable methodology to qualify smart devices, meeting SAP ESS.27 (computer-based safety systems), because of the RP's current strategy to limit the use of smart devices to SC3 and SCN.

4.3.7. Essential services

165. The BWRX-300 Safety Strategy (ref. [72]) identifies an overarching design objective to maximise the passive nature of the plant and reduce reliance on supporting systems and operator actions. SSSE Chapter 7 (ref. [2]) states that I&C systems are supported by the electrical power system and HVS.

166. SSSE Chapter 3 (ref. [3]) identifies two types of support functions. Integral support functions are required to be performed concurrently with the primary function and are assigned the same safety category as the primary function. Make-ready support functions are continuous functions that maintain the primary function in a state of readiness but are not required to be performed at the time the primary function is performed. Make-ready support functions are assigned to Safety Category 3. Monitoring of make-ready functions is required to alert operators if the function becomes unavailable.

167. The electrical power systems are the subject of a dedicated electrical assessment (ref. [113]), which considers their adequacy to support the required I&C safety functions. Electrical power is an integral support function to the I&C systems and necessary to support the delivery of I&C safety functions. The PPS is powered by the SC1 R10 Emergency Power System, which is battery backed for 72-hours. R10 comprises three independent divisions reflecting the redundancy of the PPS and is independent and physically separate from other plant electrical systems reflecting the independence required between DL3 and DL2/DL4a. The DPS is powered by the R20 Standby Power System which provides battery backed supplies in a loss of preferred power event. The components of R20 supporting the DPS are SC2. I consider the high-level architecture of the electrical power systems to be consistent with the requirements of the I&C architecture.

168. Environmental conditions for I&C equipment are maintained by HVSs:

- the PPS is supported by the RB HVS
- the DPS is supported by the CB HVS

169. The RP considers HVSs to be make-ready support systems on the basis that PPS and DPS safety functions are delivered early in the response to an event well before equipment room temperatures could exceed tolerable limits for the I&C equipment. According to the RP's categorisation and classification methodology (ref. [88]), equipment which delivers make-ready support functions are assigned to Safety Category 3.

170. In summary, I judge that the claims made and the proposed architecture of support systems satisfy SAP EES.1 (provision of essential services). However, a future BWRX-300 safety case will need to provide evidence to underpin the claims that the PPS and DPS will deliver the required safety functions with no operational HVS. A future BWRX-300 safety case will also need address the role of the PPS and DPS in delivering safety functions which are necessary after the initial response to an event, such as indicating key parameters to operators to confirm the continued operation of passive features. A future BWRX-300 safety will also need to address the risk of spurious actuation arising from HVS failures impacting PPS and DPS equipment.

4.3.8. Cyber security for safety

171. ONR's assessment of cyber security is led by cyber security and information assurance (CS&IA) (ref. [115]). I have supported this assessment to help confirm the adequacy of cyber security arrangements necessary to ensure dependable operation of I&C safety systems.

172. The RP has identified security as a fundamental design property of each I&C system. There is appropriate signposting from SSSE Chapter 7 (ref. [2]) to the cyber security chapter, SSSE Chapter 25 (ref. [10]), where the claims

and arguments are further developed and assessed as part of ONR's cyber security assessment (ref. [115]).

173. As discussed in section 4.3.4, a key aspect of my I&C assessment has been the RP's selection of an all-digital I&C architecture. In collaboration with ONR's cyber security inspector, I have sought to confirm that cyber security has been factored into decision making and that independence claims between I&C systems are not compromised by common vulnerabilities or by any measures introduced for cyber security reasons.

174. In its response to RQ-01756 (ref. [97]), the RP outlined the factors it considered in its decision to use digital technology for the DPS. The RP confirmed in its response to RQ-01903 (ref. [116]) that cyber security aspects were considered after the decision to use digital technology had been made, in a preliminary cyber risk assessment (ref. [117]). I raised RO-BWRX300-001 (ref. [94]) Action A3, which includes consideration of how secure by design has been applied in the decision making to select a digital DPS platform, and Action 4 which requires the RP to justify the technology choices within the I&C architecture with due consideration to both safety and security aspects. The RP has committed in its Resolution Plan (ref. [103]) to perform these activities to support a future BWRX-300 safety case.

175. The RP's Cyber Security Program Plan (ref. [118]) identifies a requirement to ensure that cyber security measures do not compromise the effectiveness of diversity and defence-in-depth features. This is aligned with the requirements of IEC 62859 (ref. [119]). In addition, in response to RO-BWRX300-001 Action 3 (ref. [103]), the RP has committed to explain how cyber security activities consider and support independence claims for safety.

176. In summary, while I consider there to be a gap to regulatory expectations in how cyber security aspects are considered and justified in the RP's decision to use an all-digital architecture, the RP has committed to resolving these within its RO-BWRX300-001 Resolution Plan (ref. [103]) and therefore, I do not consider there to be a fundamental shortfall with the design at this design stage.

4.3.9. Ageing management

177. At GDA Step 2, the RP has not identified any specific requirements in relation to the management of ageing, since the I&C systems design is not mature enough to identify specific ageing stressors. However, the RP has committed that these will be identified and managed, both via the implementation of the Plant Level I&C Maintenance Plan as committed within the Plant Level Instrumentation and Control Architecture Design Assurance Plan (ref. [78]) and via equipment qualification in line with the graded requirements by safety class in accordance with IEC/IEEE 60780-323 (ref. [107]).

178. Despite the limited information available at GDA Step 2 in relation to ageing management for I&C systems, it is my opinion that the RP has identified relevant codes and standards such as IEC 61513 (ref. [64]), noting that IEC 61513 refers to IEC 62342 (ref. [70]) for further guidance on management of ageing, and IEC/IEEE 60780-323 (ref. [107]) to guide the development of a future safety case. I have not identified any significant shortfalls in this area and have confidence that the BWRX-300 is likely to satisfy SAP EAD.2 (lifetime margins) in the future.

4.3.10. ALARP

179. At GDA Step 2 and recognising the current degree of design maturity, it is only possible to consider whether risks are likely to be reduced to ALARP in terms of high-level architecture, design principles and documented requirements.

180. I consider that the RP's approach to developing I&C systems is broadly consistent with the expectations of RGP. The RP has identified an appropriate set of standards and guidance, and to date its application of these benchmarks has been in line with expectations. In line with the guidance in NS-TAST-GD-005 (ref. [57]), this is a key component of an ALARP demonstration.

181. As discussed in Section 4.3.4, the RP is proposing to use digital platforms to provide the necessary independence and diversity in the I&C architecture. The actions identified under RO-BWRX300-001 (ref. [94]) will provide further confidence that an appropriate ALARP demonstration can be made in a future BWRX-300 safety case.

5. Conclusions

182. This report presents the Step 2 I&C assessment for the GDA of the BWRX-300 design. The focus of my assessment in this step was 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. [19]), at the content of most relevance to I&C against the expectations of ONR's SAPs, TAGs and other guidance which ONR regards as RGP, such as IAEA SSG-39 (ref. [62]) and IEC 61513 (ref. [64]).

183. Based upon my assessment, I have concluded the following:

- The RP's design principles are sufficiently developed and demonstrate good alignment with ONR's expectations for overall design goals. Application of the design principles has resulted in a set of fundamental design properties for each I&C system, which feed into the RP's requirements management system to be substantiated at a later design stage;
- The RP's documented set of I&C reference standards and guidance provides an appropriate benchmark for RGP;
- The RP's method for categorisation and classification is, from an I&C perspective, consistent with RGP and has been applied appropriately for key I&C systems based on the design information currently available;
- The RP has identified an appropriate set of I&C systems based on the current design information, with system reliability targets within the expected ranges consistent with their safety class. The system reliability targets selected for SC2 and SC3 systems are at the more reliable end of the expected reliability claim range, and a future BWRX-300 safety case will need to provide a stronger safety demonstration for these systems reflecting these more reliable claims;
- The high-level architecture has the potential to achieve the necessary system independence. However, there are several aspects which require further development in a future BWRX-300 design and safety case including a demonstration that spurious failures of lower class systems do not result in unnecessary demands on higher class systems and that failures within the lower class systems cannot impact the delivery of safety functions of higher class systems;
- The RP has indicated that it intends to use an all-digital I&C architecture. I raised RO-BWRX300-001 as, in my opinion, the RP had down selected credible I&C platform technology options before it has demonstrated its preferred design solution can achieve the relevant

safety and security expectations. In addition, the strategic decisions, design principles and supporting processes which underpin high level diversity claims are not, in my opinion, clearly identified which makes it unclear if a future safety case will be able to substantiate these claims. The RP has committed to resolving these aspects within its Resolution Plan (ref. [103]) and therefore, I do not consider this to be a fundamental shortfall with the design at this design stage;

- The 2-out-of-3 voting logic of the SC1 PPS satisfies the single failure criterion for most plant states. However, it does not comply with the single failure criterion when a maintenance bypass is applied. This does not meet the expectations of IAEA SSG-39, which requires the single failure criterion to be met in all permissible plant states, including where part of the safety system is bypassed. The RP presented a justification within RQ-01757 which relies on the extent of diagnostic and self-test features within the PPS, the overall equipment failure rate being very low and the implementation of suitable technical specifications to limit the time at risk. A future BWRX-300 design and safety case will need to develop and substantiate the claims in this area;

- The BWRX-300 HMI design supports the I&C systems and the delivery of identified human actions at this stage of the design. Future design activities, such as system level failure modes and effects analyses, may result in the identification of further requirements for HMIs. The BWRX-300 design has no high-integrity displays at present due to there being no identified need. A future BWRX-300 design and safety case will need to confirm that high-integrity displays and indications are not required once all human actions are identified;

- The RP has established and begun implementing an adequate framework for I&C functional and property claims;

- The RP has set out high level plans for how it intends to perform the safety demonstration of the I&C systems using the PE and ICBM framework. These plans are high-level and will need to be developed to support a future BWRX-300 safety case;

- Requirements and indicative high-level architecture for essential systems for I&C, namely electrical power supplies and HVS, meet ONR expectations for I&C at this stage of the design. A future BWRX-300 design and safety case will need to substantiate claims which decouple HVS failures from the delivery of I&C safety functions;

- The RP has established high level interfaces between the I&C design and cyber security design processes;

- The RP has identified the need to develop plans for the management of ageing of I&C equipment and has identified RGP which supports these aims; and,

- The RP's development of its I&C systems is broadly consistent with the expectations of UK and international RGP, which provides a sound basis to reduce risks to ALARP.

184. 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 and to the resolution of RO-BWRX300-001, 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.

6. References

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

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

[3] GE-Hitachi, NEDO-34165 BWRX-300 UK GDA Chapter 3 - Safety Objectives and Design Rules for SSCs, Rev C, 15 July 2025, ONRW-2019369590-22497.

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

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

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

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

[8] GE-Hitachi, NEDO-34178 BWRX-300 UK GDA Chapter 15 - Safety Analysis, Rev B, 11 July 2025, ONRW-2019369590-22392.

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

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

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

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

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

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

https://www.onr.org.uk/media/z5mnnigr/onr-rd-pol-002-risk-informed-and-targeted-engagements-rite-policy.docx.

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

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

[17] ONR, NS-TAST-GD-108, Guidance on the Production of Reports for Permissioning and Assessment, Issue No. 2, December 2023, Record ref. 2022/71935, www.onr.org.uk/operational/tech_asst_guides/index.htm.

[18] ONR, ONR-GDA-GD-006, New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, Issue 1, August 2024, https://www.onr.org.uk/media/iexmextu/onr-gda-gd-006.docx.

[19] ONR, Step 2 Control and Instrumentation Assessment Plan for the Generic Design Assessment of the GE Hitachi BWRX-300, Issue 1, December 2024, ONRW-2126615823-4539.

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

[21] GE-Hitachi, NEDO-34163 BWRX-300 UK GDA Chapter 1 - Introduction, Rev B, 11 July 2025, ONRW-2019369590-22413.

[22] GE-Hitachi, NEDO-34164 BWRX-300 UK GDA Chapter 2 - Site Characteristics, Rev B, 15 July 2025, ONRW-2019369590-22496.

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

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

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

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

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

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

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

[30] GE-Hitachi, NEDO-34179 BWRX-300 UK GDA Chapter 15.1 - Safety Analysis - General Considerations, Rev B, 11 July 2025, ONRW-2019369590-22391.

[31] GE-Hitachi, NEDO-34180 BWRX-300 UK GDA Chapter 15.2 - Identification Categorization Grouping of PIEs and Accident Scenarios, Rev B, 15 July 2025, ONRW-2019369590-22505.

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

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

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

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

[36] GE-Hitachi, NEDO-34185 BWRX-300 UK GDA Chapter 15.7 - Analysis of Internal Hazard, Rev B, 15 July 2025, ONRW-2019369590-22510.

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

[38] 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.

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

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

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

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

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

[47] GE-Hitachi, NEDO-34198 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, Rev 2, September 2024, ONRW-2019369590-13525.

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

[51] ONR, ONR-CNSS-MAN-001, ONR Nuclear Material Accountancy, Control, and Safeguards Assessment Principles (ONMACS), Issue No. 5, February 2022. www.onr.org.uk/operational/other/onr-cnss-man-001.pdf.

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

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

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

[55] WENRA, 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.

[56] ONR, NS-TAST-GD-003, Safety Systems, Issue 9.3, December 2024, www.onr.org.uk/operational/tech_asst_guides/index.htm.

[57] 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.

[58] ONR, NS-TAST-GD-046, Computer based safety systems, Issue 7, December 2023, www.onr.org.uk/operational/tech_asst_guides/index.htm.

[59] ONR, NS-TAST-GD-094, Categorisation of safety functions and classification of structures, systems and components, Rev 2, July 2019. www.onr.org.uk/media/documents/guidance/ns-tast-gd-094.pdf.

[60] IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1, Revision 1. February 2016, www.iaea.org.

[61] IAEA, Safety classification of structures, systems and components in nuclear power plants, Specific safety guide no SSG-30, 2014. www.iaea.org.

[62] IAEA, Design of instrumentation and control systems for nuclear power plants, specific safety guide no SSG-39, 2016. www.iaea.org.

[63] IEC, Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorisation of functions and classification of systems, IEC 61226, 2020. www.iec.ch.

[64] IEC, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, IEC 61513, 2011, www.iec.ch.

[65] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions, IEC 60880, 2006, www.iec.ch.

[66] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions, IEC 62138, 2018, www.iec.ch.

[67] IEC, Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions, IEC 62566, 2012, www.iec.ch.

[68] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Development of HDL-programmed integrated circuits - Part 2: HDL-programmed integrated circuits for systems performing category B or C functions, IEC 62566-2, 2020, www.iec.ch.

[69] IEC, Nuclear power plants - Instrumentation and control important to safety - Hardware requirements, IEC 60987, 2021, www.iec.ch.

[70] IEC, Nuclear power plants - Instrumentation and control systems important to safety - Management of ageing, IEC 62342, 2007, www.iec.ch.

[71] Task Force on Safety Critical Software, Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations, Revision 2022. www.onr.org.uk/software.pdf.

[72] GE-Hitachi, 006N5064 BWRX-300 Safety Strategy, Rev 6, ONRW-2019369590-14013.

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

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

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

[76] IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants, Specific Safety Guide No. SSG-61, September 2021. www.iaea.org.

[77] GE-Hitachi, 006N5199 BWRX-300 Plant Instrumentation and Control Systems Nuclear Regulations and Standards Compliance Plan, Rev 2, August 2024, ONRW-2019369590-21871.

[78] GE-Hitachi, 006N2631 BWRX-300 Plant Level Instrumentation and Control Architecture Design Assurance Plan, Rev 2, July 2023, ONRW-2019369590-14873.

[79] GE-Hitachi, 006N5114 BWRX-300 Plant I&C Systems Architecture Requirements and Design, Rev 2, ONRW-2019369590-21872.

[80] GE-Hitachi, 006N5991 BWRX-300 Plant Architecture Definition, Rev 0, ONRW-2019369590-14828.

[81] GE-Hitachi, 007N5107 BWRX-300 I&C Failure Mode and Hazards Analyses Plan, Rev B, July 2024, ONRW-609516046-1754.

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

[83] 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/.

[84] GE-Hitachi, 005N9036 BWRX-300 Requirements Management Plan, Rev 6, April 2024, ONRW-2019369590-17795.

[85] GE-Hitachi, M250037, Submission of BWRX-300 UK GDA Step 2 Regulatory Query (RQ)-01743 Full Response, 28 March 2025, ONRW-609516046-1261.

[86] GE-Hitachi, M250216, Submission of BWRX-300 UK GDA Step 2 RQ-02005 Response, 9 May 2025, ONRW-609516046-1825.

[87] GE-Hitachi, 006N3139 BWRX-300 Design Plan, Rev 5, December 2023, ONRW-2019369590-14011.

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

[89] ONR, AR-01348, Generic Design Assessment of the BWRX-300 – Step 2 assessment of Fault Studies including Severe Accident, Issue 1, December 2025, ONRW-2126615823-7646.

[90] GE-Hitachi, 005N3558 BWRX-300 Fault Evaluation, Rev 3, ONRW-2019369590-14870.

[91] GE-Hitachi, M250195, Submission of BWRX-300 UK GDA GEH Response to Regulatory Query RQ-01875, 2 May 2025, ONRW-2019369590-20339.

[92] GE-Hitachi, NEDC-34274P BWRX-300 UK GDA Forward Action Plan, Rev 2, July 2025, ONRW-2019369590-22522.

[93] GE Hitachi, M250330, Submission of BWRX-300 UK GDA – Response to RQ-02425, 9 October 2025, ONRW-609516046-3292.

[94] ONR, RO-BWRX300-001, Demonstration of independence and diversity in the BWRX-300 I&C architecture, Revision 1.0, 20 June 2025, ONRW-2126615823-7689.

[95] ONR, RO-ABWR-0077, Demonstration of adequate protection for Pellet-cladding Interaction in response to Control-rod Movement Faults, 16 December 2016, 2016/431381, https://www.onr.org.uk/media/nqklh3s3/ro-abwr-0077.pdf.

[96] ONR, ONR-NR-CR-24-775, GE Hitachi BWRX-300 GDA – Step 2 – Control and Instrumentation L4 Meeting, Issue 1, 25 February 2025, ONRW-2019369590-18349.

[97] GE-Hitachi, M250047, Submission of BWRX-300 UK GDA Step 2 RQ-01756 Response, 25 March 2025, ONRW-609516046-1198.

[98] GE-Hitachi, M250170, Submission of BWRX-300 UK GDA, Regulatory Query (RQ)-01961 Response, 2 May 2025, ONRW-609516046-1721.

[99] Lawrence Livermore National Laboratory, NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, December 1994, https://www.nrc.gov/docs/ML0717/ML071790509.pdf.

[100] Oak Ridge National Laboratory, NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, December 2008, https://www.nrc.gov/docs/ML1005/ML100541256.pdf.

[101] GE-Hitachi, 008N1105, Safety Class 2 H20 Diverse Protection System Platform Suitability Assessment, Revision A, December 2023, ONRW-609516046-1724.

[102] US NRC, NUREG-0800, Branch Technical Position 7-19, Guidance for evaluation of defense in depth and diversity to address common-cause failure due to latent design defects in digital safety systems, Revision 8, January 2021, https://www.nrc.gov/docs/ML2033/ML20339.

[103] GE-Hitachi, M250288, Submission of BWRX-300 UK GDA RO-BWRX300-001 Resolution Plan, 11 July 2025, ONRW-2126615823-7938.

[104] GE-Hitachi, M250315, Submission of BWRX-300 UK GDA, RO-BWRX300-001 Delivery Plan, 29 August 2025, ONRW-2126615823-8533.

[105] GE-Hitachi, M250163, Submission of BWRX-300 UK GDA Regulatory Query (RQ)-01937 Full Response, 15 April 2025, ONRW-609516046-1474.

[106] ONR, AR-01354, Generic Design Assessment of the BWRX-300 – Step 2 assessment of Internal Hazards, Issue 1, December 2025, ONRW-2126615823-4321.

[107] IEC, Nuclear facilities - Electrical equipment important to safety - Qualification, IEC/IEEE 60780-323, 2016, www.iec.ch.

[108] IEC, Nuclear facilities - Equipment important to safety - Seismic qualification, IEC/IEEE 60980-344, 2020, www.iec.ch.

[109] GE-Hitachi, M250048, Submission of BWRX-300 UK GDA Step 2 RQ-01757 Response, 14 March 2025, ONRW-609516046-1079.

[110] IEEE, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603, 27 September 2018, standards.ieee.org.

[111] ONR, ONR-NR-CR-25-069, GE Hitachi BWRX-300 GDA – Step 2 – Control and Instrumentation L4 Meeting, 30 April 2025, Issue 1, ONRW-2019369590-20463.

[112] IEC, Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality, IEC 62671, 2013, www.iec.ch.

[113] ONR, AR-01367, Generic Design Assessment of the BWRX-300 – Step 2 assessment of Electrical Engineering, Issue 1, December 2025, ONRW-2126615823-7654.

[114] GE-Hitachi, M250104, Submission of BWRX-300 UK GDA Regulatory Query (RQ)-01844, Full Response, 30 April 2025, ONRW-609516046-1635.

[115] ONR, AR-01359, Generic Design Assessment of the BWRX-300 – Step 2 assessement of Cyber Security, Issue 1, December 2025, ONRW-2126615823-7836.

[116] GE-Hitachi, M250144, Submission of BWRX-300 UK GDA GEH Response to RE-01903, 29 April 2025, ONRW-609516046-1606.

[117] GE-Hitachi, 008N5815 BWRX-300 C20 Diverse Protection System Cyber Security Assessment Report, Rev A, May 2024, ONRW-609516046-1600.

[118] GE-Hitachi, 006N6731 BWRX-300 Plant Cyber Security Program Plan, Rev 2, August 2023, ONRW-2019369590-14763.

[119] IEC, Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity, IEC 62859, 2016, www.iec.ch.

Appendix 1 – Relevant SAPs considered during the assessment

SAP reference	SAP title
EAD.2	Ageing and degradation – Lifetime margins
ECS.1	Safety classification and standards – Safety categorisation
ECS.2	Safety classification and standards – Safety classification of SSCs
ECS.3	Safety classification and standards – Codes and standards
EDR.2	Design for reliability – Redundancy, diversity and segregation
EDR.3	Design for reliability – Common cause failure
EDR.4	Design for reliability – Single failure criterion
EES.1	Essential services – Provision
EHF.7	Human factors – User interfaces
EKP.3	Key principles – Defence in depth
EKP.5	Key principles – Safety measures
ELO.4	Layout – Minimisation of the effects of incidents
ERL.1	Reliability claims – Form of claims
ESS.1	Safety systems – Provision of safety systems
ESS.2	Safety systems – Safety system specification
ESS.13	Safety systems – Confirmation to operating personnel
ESS.18	Safety systems – Failure independence
ESS.20	Safety systems – Avoidance of connections to other systems
ESS.27	Safety systems – Computer based safety systems
SC.2	Safety cases – Safety case process outputs