Office for Nuclear Regulation

ONR Assessment Report

Generic Design Assessment of the BWRX-300 – Step 2 Assessment of Cyber Security

ONR Assessment Report

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

Report Title: Step 2 Assessment of Cyber Security

Authored by: Embedded TSC, Nuclear Security, ONR

Principal Inspector, Nuclear Security, ONR

Assessment report reference: AR-01359

Project report reference: PR-01880

Report issue: 1

Published: December 2025

Document ID: ONRW-2126615823-8404

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 cyber security assessment of the BWRX-300 design as part of Step 2 of the ONR GDA. This assessment is based upon the information presented in the RP's safety, security, safeguards and environment cases (SSSE), the associated revision 3 of the Design Reference Report and supporting documentation.

ONR's GDA process calls for an assessment of the RP's submissions. The focus of my assessment in this step was to support ONR's decision on the fundamental adequacy of the BWRX-300 design and security 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 Security Assessment Principles (SyAPs), Technical Assessment Guides (TAGs) and other guidance which ONR regards as relevant good practice, such as International Atomic Energy Agency security 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:

- Cyber Security Assessment Process;
- Defensive Cyber Security Architecture;
- Incorporation of Secure by Design;
- Independence and Diversity of Safety Systems; and
- Plant Cyber Security Program Plan

In line with the objectives for Step 2, I undertook a broad review of the highest level, fundamental claims and supporting arguments related to cyber security. My expectations for Step 2 GDA were that the RP would demonstrate its approach to analysis of cyber risks to the design by identifying, characterising and assessing the relevant systems to demonstrate they can be appropriately protected.

The focus of my assessment was the fundamental adequacy of the cyber security risk assessment methodology and a demonstration of its application against the

design. This would allow the RP to demonstrate in GDA that cyber security risks to the design will be identified and assessed to inform the design of a Cyber Protection System (CPS) as part of the overall security justification. The methodology took into account the cyber threats described in the RP's proxy Design Basis Threat (DBT), which is reasonable and contains generally accepted threats to inform and evaluate its CPS design, and the risk assessment methodology demonstrated that the relevant CPS outcomes defined in SyAPs could be met.

I found that the RP was proportionate and diligent in the approach to cyber security, with a willingness to address challenges to design and methodology which gave me confidence that the forward action plans put in place would address site-specific requirements as required.

The RP has indicated that it intends to use an all-digital control and instrumentation architecture. RO-BWRX300-01 has been raised by the control and instrumentation inspector to seek confidence that relevant safety and security expectations are met. The RP has committed to carry out further work, as defined in its Resolution Plan, to substantiate its design decision, including consideration of how cyber security supports the principle of independence and how secure by design principles are applied in this design decision making.

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

List of abbreviations

ALARP	As Low as Reasonably Practicable
ABWR	Advanced Boiler Water Reactor
BL	Baseline
BWR	Boiling Water Reactor
CBSIS	Computer-Based System Important to Safety
CEA	Cyber Essential Assets
CNSC	Canadian Nuclear Safety Commission
CPS	Cyber Protection System
CSAP	Cyber Security Assessment Process
CSAR	Cyber Security Assessment Report
CS&IA	Cyber Security & Information Assurance
CySPP	Cyber Security Program Plan
DAC	Design Acceptance Confirmation
DBT	Design Basis Threat
DCSA	Defensive Cyber Security Architecture
DMZ	De-Militarised Zone
DPS	Diverse Protection System
DRR	Design Reference Report
ESBWR	Economic Simplified Boiling Water Reactor
GB	Great Britain
GDA	Generic Design Assessment
GVHA	GE Vernova Hitachi Nuclear Energy Americas LLC
IAEA	International Atomic Energy Agency
IAM	Identity and Access Management
I&C	Instrumentation and Control
KSyPP	Key Security Plan Principle
MDSL	Master Document Submission List
NISR	Nuclear Industries Security Regulations
NM	Nuclear Material
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
ONR	Office for Nuclear Regulation
ORM	Other Radioactive Material
PA	Protected Area
PER	Preliminary Environmental Report
PPS	Physical Protection System
PSAR	Preliminary Safety Analysis Report
PSR	Preliminary Safety Report
RBAC	Role-Based Access Control
RGP	Relevant Good Practice
RITE	Risk Informed Targeted Engagement
RO	Regulatory Observation
RP	Requesting Party
RPV	Reactor Pressure Vessel
RQ	Regulatory Query

SBD	Secure by Design
SBWR	Simplified Boiling Water Reactor
SL-T	Security Level - Target
SMR	Small Modular Reactor
SNI	Sensitive Nuclear Information
SSCs	Structures, Systems and Components
SSSE	Safety, Security, Safeguards and Environment Cases
STAR	Sabotage, Target Analysis and Review
SUC	System Under Consideration
SyAPs	Security Assessment Principles
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide(s) (ONR)
TSC	Technical Support Contractor
UK	United Kingdom
US	United States of America
VAI	Vital Area Identification
WENRA	Western European Nuclear Regulators' Association

Contents

1. Introduction

1. This report presents the outcome of the cyber security 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 (ref. [1]), specifically chapters 7 (ref. [2]) and 25 (ref. [3]), the associated revision of the Design Reference Report (DRR) (ref. [4]) 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. [5]) and ONR's risk informed, targeted engagements (RITE) guidance (ref. [6]). The ONR Security Assessment Principles (ref. [7]) together with supporting Technical Assessment Guides (TAGs) (ref. [8]), 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. [9])).

1.1. Background

4. The ONR's GDA process (ref. [10]) 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 Safety, Security, Safeguards and Environment cases (SSSE), and other technical documents for the GDA.

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

8. Step 1 is the preparatory part of the design assessment process and is mainly associated with initiation of the project and preparation for technical assessment in Step 2. Step 1 completed in December 2024. Step 2 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 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 security (ref. [11]). 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. [12]) and published on the regulators' website.

1.2. Scope

14. The assessment documented in this report is based upon the SSSE for the BWRX-300 (refs. [1], [13], [14], [15], [16], [17], [18], [2], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28] [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [3], [46], [47], [48]).

15. 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. [4]) and the 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 nuclear power plant (NPP) that is proposed for consideration in the GDA. DRR provides a list of the systems, structures and components (SSCs) which are included in the scope of the GDA, and their relevant GDA reference design documents.

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

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

18. The regulatory conclusions from GDA apply to everything that is within the GDA scope. However, ONR does not assess everything within it or all matters to the same level of detail. This applies equally to my own assessment, and I have followed ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [5]) and ONR's guidance on Risk Informed, Targeted Engagements (ref. [6]).

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

- Specific technology choices related to security systems. These will be determined by GVHA and any future GB developers once the UK Design Basis Threat (DBT) has been applied, the relevant Physical Protection System (PPS) and Cyber Protection System (CPS) outcomes have been confirmed and site specific characteristics taken into account;

- Instructions and concept of operations for security and operational staff and response forces. These will be developed by a licensee in conjunction with relevant bodies and determined by the security outcome once Vital Area Identification (VAI) has been undertaken using the UK DBT; and

- Cyber security arrangements outside of plant control systems and networks, in particular, enterprise measures to secure corporate networks.

20. My assessment has considered the following aspects:

- The adequacy of the RP's methodology and approach to Secure by Design (SbD);

- The RP's approach to demonstrating defence-in-depth for cyber security within the Defensive Cyber Security Architecture (DCSA) (ref. [51]);

- The adequacy of the RP's Cyber Security Assessment Process;

- The RP's approach to independence and diversity of safety systems; and

- Confidence that the design is capable of enabling a future licensee to deliver an approved security plan that complies with the Nuclear Industries Security Regulations (NISR) 2003, via an appropriate program plan or similar.

21. This report contains sensitive nuclear information (SNI) relating to the assessment of the RP's defensive cyber security architecture. This has been appended to allow for the main body of the report to remain as "OFFICIAL" information and releasable to the public. This information has been categorised in line with the Classification Policy for the Civil Nuclear Industry (ref. [52]). In accordance with Section 79 of the Anti-Terrorism, Crime and Security Act (ref. [53]), the information in Appendix 2 is not made available to the public and has been removed from the publicly accessible version of this report.

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 Security Assessment Principles (SyAPs) (ref. [7]) constitute the regulatory principles against which the RP's case is judged. Consequently, the SyAPs 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. [54]) and nuclear security series (ref. [55]) 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. [56]), which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors (ref. [57]).

27. The relevant SyAPs and IAEA standards are embodied and expanded on in the TAGs (ref. [8]). The TAGs provide the principal means for assessing the cyber security aspects in practice.

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

2.1.1. Security Assessment Principles (SyAPs)

29. The key assessment principles used in this cyber security assessment is Fundamental Security Principle (FSyP) 7 - Cyber Security and Information Assurance. This has formed the basis of my assessment to ensure that the RP has implemented and maintained effective cyber security and information assurance arrangements that integrate technical and procedural controls to protect the confidentiality, integrity and availability of SNI and technology. To provide a judgement on the fundamental adequacy of the RP's CPSs, I have drawn upon the following supporting SyAPs Annexes,

Security Delivery Principles (SyDPs) and Key Security Plan Principles (KSyPPs):

- SyDP 7.1 – Effective Cyber and Information Risk Management
- SyDP 7.3 – Protection of Nuclear Technology and Operations
- KSyPP 1 – Secure by Design
- KSyPP 2 – The Threat
- KSyPP 3 – The Graded Approach
- KSyPP 4 – Defence-in-Depth
- Annex H – Cyber Protection System Outcomes

30. A list of the SyAPs used in this assessment is recorded in Appendix 1.

2.1.2. Technical Assessment Guides (TAGs)

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

- CNS-TAST-GD-11.4.1 – Secure by Design [58]
- CNS-TAST-GD-11.1 - Guidance on the Security Assessment of Generic New Nuclear Reactor Designs [59]
- CNS-TAST-GD-7.1 - Effective Cyber and Information Risk Management [60]
- CNS-TAST-GD-7.3 – Protection of Nuclear Technology and Operations [61]

2.1.3. National and international standards and guidance

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

- ISA/IEC 62443 – Security for Industrial Automation and Control Systems [62]
- NIST 800 – 82 rev3 – Guide to Operational Technology Security [63]
- ISO 27001:2022 – Information Security Management Systems [64]

2.2. Integration with other assessment topics

33. I have worked closely with other topics as part of my security assessment. Similarly, other assessors saw input from my assessment. These interactions are key to prevent or mitigate any gaps duplications or

inconsistencies in ONR's assessment. The key interactions with other topic areas were:

- **Sabotage, Target Analysis and Review (STAR)**. The VAI process is a key activity required to ensure those SSCs requiring protection have been adequately identified and proportionate security arrangements have been adopted to protect those areas. I have worked closely with the STAR inspector discussing the nature and efficacy of blended attack scenarios in respect of the RP's design.

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

- **Protective Security.** I have worked closely with the protective security inspector to ensure that those areas containing computer based systems important to safety (CBSIS) and security systems have appropriate physical protection in place.

2.3. Use of technical support contractors

34. ONR has engaged a Technical Support Contractor (TSC) who was embedded in ONR to deliver the assessment of the cyber security aspects of the BWRX-300 GDA. It should be noted that all regulatory judgements have been made exclusively by ONR.

3. Requesting Party's submission

35. 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.

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

37. This section presents a summary of the RP's cyber security case. It also identifies the documents submitted by the RP which have formed the basis of my Step 2 assessment of the BWRX-300 design.

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

3.1. Summary of the BWRX-300 Design

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

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

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. [16]).

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.

43. The reactor is located within the power block, which itself is located within a protected area, which the RP have included in its security case.

3.2. BWRX-300 Case Approach and Structure

44. The RP has submitted information on its strategy and intentions regarding the development of the SSSE (refs [65], [66], [67], [68]). This was submitted to ONR during Step 1.

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

46. The format and structure of the PSR largely aligns with the IAEA guidance for safety cases, SSG-61 (ref. [69]), supplemented to include a specific chapter for security. The RP has also provided a chapter on As Low as Reasonably Practicable (ALARP), which is applicable to all safety chapters. The RP has stated that the design and analysis referenced in the PSR is consistent with the March 2024 Preliminary Safety Analysis Report (PSAR) submitted to the US Nuclear Regulatory Commission (NRC). The Security Assessment and PER are for the same March 2024 design but have more limited links to any US or Canadian submissions.

3.3. Summary of the RP's case for Security

47. The RP's security case is documented in the BWRX-300 Security Assessment, which provides a holistic approach to security. This encompasses both physical security and cyber security measures, designed to protect identified safety SSCs against malevolent acts through the application of physical and cyber security measures to ensure:

- The ability to shut down the reactor and maintain sub-criticality;
- The ability to cool irradiated fuel, both in the core and in the spent fuel pool; and
- Prevention, or ability to limit release, of radioactivity affecting public safety.

3.3.1. Secure by Design

48. The RP has adopted a SbD approach through the identification of those safety SSCs requiring protection, identifying SSCs that it claims provide inherent security and mitigation against threats and designing a PPS and CPS that mitigates additional vulnerabilities identified through adversarial pathway analysis.

3.3.2. Cyber Security

49. The RP has put in place a Cyber Security Program intended to demonstrate its approach to analysis of cyber risks to the design by a process of identification, characterisation and assessment of relevant systems to demonstrate that they can be appropriately protected.

3.3.3. Design Basis Threat

50. The RP has developed a 'proxy' DBT that it considers establishes a set of credible characteristics, capabilities and techniques for the theft and/or sabotage of nuclear material (NM) or other radioactive material (ORM) to provide assurance that a country specific DBT is capable of being successfully applied to the standard design without significant changes to that design.

3.4. Basis of assessment: RP's documentation

51. The principal documents that have formed the basis of my cyber security assessment of the SSSE are:

- Chapter 25 – Security Annex of the PSR which outlines the security case (ref. [3]);
- Chapter 7 – The C&I Annex of the PSR (ref. [2]);
- The RP's Security Assessment Document (ref. [70]);
- BWRX-300 System Cyber Security Assessment Process (ref. [71]);
- BWRX-300 Defensive Cyber Security Architecture (ref. [72]);
- BWRX-300 Plant Cyber Security Program Plan (ref. [73]);
- BWRX-300 Cyber Security Controls for the Software Development Lifecycle (ref. [74]);
- C10 BWRX-300 Primary Protection System Cyber Security Assessment Report (CSAR) (ref. [75]);
- C20 Diverse Protection System Cyber Security Assessment Report (ref. [76]);

- C34 Electrical Power Supply Control System Cyber Security Assessment Report (ref. [77]);
- Forward Action Plan (ref. [78]), which captures the RP's commitments required in order to progress to GDA Step 3 or to a site specific phase; and
- BWRX-300 Plant Instrumentation and Control Digital Systems and Software Process Engineering Software QA Program Plan (ref. [79])

52. The Security Assessment (ref. [70]) consists of an overarching narrative which includes an executive summary, scope, applicable standards and guidance, site characteristics, key plant systems, RP's assessment methodology, defensive strategy, human factors engineering for security and software tools. These are supported in more detail by appendices listed as follows:

- Appendix A – BWRX-300 Security Design Basis Threat
- Appendix B – Tables and Figures
- Appendix C – Vulnerability Analysis
- Appendix D – Vital Equipment and Vital Areas
- Appendix E – Target Set Analysis
- Appendix F – Blast and Breaching Analysis
- Appendix G – Security Computer System Cybersecurity Plan
- Appendix H – Defensive Strategies
- Appendix I – Preliminary Staffing Analysis
- Appendix J – Preliminary Engagement Analysis
- Appendix K – Scenarios
- Appendix L – Aircraft Impact Structural Response Analysis
- Appendix M – Physical Protection System Design Requirements
- Appendix N – Cross-Reference to Requirements

3.5. Design Maturity

53. My assessment is based on revision 3 of the DRR (ref. [4]). 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.

54. The reactor building and the turbine building, along with the majority of the significant SSCs are housed with 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.

55. 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).

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

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

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

58. The CPS design and DCSA have been developed with the aim to provide defence in depth protection to those significant safety SSCs that have been identified as Cyber Essential Assets (CEAs) during the identification process underpinned by the Cyber Security Assessment Process (CSAP). However, it is important to note that the CPS has been developed to mitigate threats documented within the RP's own proxy DBT.

4. ONR assessment

4.1. Assessment strategy

59. 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 cyber security as described in sections 1 and 3 of this report. My assessment strategy is set out in this section and defines how I have chosen which matters to target for assessment. My assessment is consistent with the delivery strategy for the BWRX-300 GDA [80].

60. 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). It is proposing a standard BWRX-300 design for global deployment with minimal design variations from country to country.

61. 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. [81]). Due to a number of specific security related factors, I did not identify any areas where the design, methodologies, processes, or regulatory conclusions would be appropriate to the BWRX-300 design. Primarily, these factors related to the use of the RP's proxy DBT, a different regulatory framework for security, the compact nature of the design and its impact on the physical and cyber protection system.

62. My assessment has involved engagement with the RP's security team to understand its underpinning security strategy and the methodologies it has adopted to develop the CPS. Where necessary, I have sought clarification through the issue of regulatory queries (RQs).

4.2. Assessment Scope

63. 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.

64. 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.

65. 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 cyber security. 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.

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

- **Plant Cyber Security Program Plan.** I assessed whether the RP had a cyber security program in place with a view to developing a cyber security management system;
- **Cyber Security Assessment Process.** I assessed whether the RP has adequate methodologies in place for assessment of CEA's Threats and Vulnerabilities. Also, I wanted to gain confidence that the process is repeatable for any UK specific security requirements, for example, post UK DBT application;
- **Cyber Security Risk Analysis**. I assessed the RP's methodology for identifying and mitigating cyber security risks and its application against sample CBSIS so to evidence its efficacy against SyAPs expectations, which included a consideration of cyber security impact on I&C independence and diversity of safety systems; and
- **Defensive Cyber Security Architecture.** I assessed the adequacy of the RP's methodology and processes underpinning its SbD approach and how this has influenced the design itself for security benefit either through intrinsic design solutions or the adoption of extrinsic measures.

4.3. Assessment

4.3.1. Plant Cyber Security Program Plan

67. My expectation is for the RP to develop a plan or approach to determine how it intends to meet the requirements of NISR 2003, and to identify and maintain arrangements required for effective CS&IA risk management. Effective CS&IA risk management should encompass, as recommended in TAG 7.1, all relevant aspects of:

- preparing the organisation and establishing context for risk management
- asset identification and classification
- risk assessment, identification, and treatment
- achieving the cyber security posture and managing risk to approved tolerance
- resilience and assurance of controls
- ongoing assessment, monitoring and communication
- adaption of posture in response to changes to the threat and/or organisational appetite as appropriate (ref. [60])

68. To support these expectations, the RP has created the BWRX-300 Plant Cyber Security Program Plan (CySPP) (ref. [73]) which provides a program approach to the design and protection of I&C infrastructure from a cyber perspective, and describes the RP's cyber security plan and methodology to support the design, operation and protection of the BWRX-300.

69. The CySPP is described as "Conceptual" at this step of the GDA and references US, Canadian and international standards and frameworks upon which the program is based. I sampled the suite of controls and found it to be comprehensive, including, but not limited to:

- policies and procedures
- roles and responsibilities
- interfaces with other programs
- cyber security awareness and training
- identification and classification of CEAs
- supply chain and procurement
- cyber security controls
- defence cyber security architecture
- incident response, recovery, and reporting
- secure software development lifecycle
- program evaluation, review, and maintenance

70. The CySPP sets the context of the organisation and defines its approach to cyber security risk management. It highlights the standards that have been used to this point in the design development, and establishes how digital I&C, at a high-level, will be protected. It defines key roles and responsibilities for those within the organisation who have cyber security responsibility, and defines the interfaces with other programs, such as physical security, personnel security and human factors engineering.

71. The CySPP establishes the arrangements for asset identification, including defining cyber assets and asset owners. I sampled the criteria for inclusion for cyber assets, which are adequate. A baseline set of controls to be applied to all assets have been identified, and the CySPP requires further analysis of control sets to be applied to higher risk CEAs, with verification and validation processes defined to ensure requirements are met. Requirements include, but are not limited to, those related to the

management of supply chain risk. In particular, the RP has sought to ensure a secure software development lifecycle and development environment. I judge that the RP has achieved defence in depth at a fundamental level (KSyPP4) in its security controls and will implement a system of controls based on the graded approach (KSyPP3) by implementing additional controls for higher risk assets.

72. The importance of ongoing review and maintenance is considered, with frequency and triggers identified for review of the CySPP, including changes in threat and cyber security incidents. I recommend that this element of the CySPP is updated to reflect any findings from this GDA, including ongoing commitments made to ONR.

73. I found the CySPP to be coherent, clear and, address the key elements of a cyber security plan expected to facilitate the overall aim of meeting the expectations in SyAPs and achieving the specified CPS outcomes.

74. I judge the CySPP to be fundamentally adequate and meets regulatory expectations for Step 2 of GDA.

4.3.2. Cyber Security Assessment Process

75. My expectation is for a defined and proven methodology that sets out a clear, coherent and repeatable process for identification, assessment and management of potential cyber security risks to the design. The methodology should demonstrate fundamental adequacy in the application of FSyP7, specifically SyDPs 7.1 and 7.3, and KSyPP 1-4 of SyAPs. It should also provide a credible means of meeting the outcomes for a CPS via the selection of a comprehensive set of controls. The methodology should incorporate the SbD approach and an understanding of safety requirements (in regard to CBSIS) to allow early identification of CEAs.

76. The RP's CSAP (ref. [71]) sets out a process to allow responsible engineers to perform a cyber security assessment on its digital I&C systems and components to determine the appropriate cyber security controls necessary to ensure confidentiality, integrity and availability.

77. This process is intended to allow for a high assurance that CEAs and information networks are protected against cyber-attacks and threats up to and including the UK DBT.

78. Protection systems should be designed, evaluated and tested using the state's Design Basis Threat (ref. [58]). The RP did not have access to the UK DBT during this GDA so it produced a 'proxy' DBT that it considers establishes a set of credible characteristics, capabilities and techniques, with the aim to provide assurance that they can apply the UK DBT later to the standard design without significant design changes.

79. I have reviewed the RP's proxy DBT to understand its characteristics and I am satisfied that it contains generally accepted threat types that can be used

to appropriately inform its CPS design. The RP's PSR, Chapter 25 (ref. [3]), commits the RP to using the UK DBT beyond Step 2 of the GDA, and I am satisfied the RP has adequately committed this to its Forward Action Plan (ref. [78]).

80. The CSAP methodology itself consists of a 5-step process:

- identification of cyber assets
- identification of CEAs
- classification of CEAs based on safety & security significance and susceptibility to cyber threats
- application of security controls
- submission of cyber security assessment reports for documentation and verification

81. I noted that the CSAP references NIST SP 800-82, Rev. 2, Guide to Industrial Control Systems (ICS) Security (ref. [82]). Rev 2 has since been superseded by Rev 3 (Sept 2023). NIST SP 800-82, Rev 3 aligns itself with the ISA/IEC 62443-3-2 standard for Security Risk Assessment for System Design, though I noted no reference to this international standard. Whilst the absence of reference to the ISA/IEC 62443 within the CSAP does not in itself necessarily constitute a shortfall, the risk assessment methodology within ISA/IEC 62443-3-2 is specifically identified in NIST SP 800-82, Rev 3 (6.1.3. Risk Assessment (ID.RA)) as appropriate guidance in Operational Technology environments, where risks and impacts may be related to safety, health, and the environment.

82. The CSAP draws upon multiple referenced standards to facilitate the identification and classification of: individual cyber assets; a group of similar cyber assets within a system; or a system containing one or more cyber assets based upon the consequence of compromise model. Similar cyber assets within a system that receive the same classification can be grouped together in this approach. Similar cyber assets within a system that receive different classifications are not to be grouped together and have separate classification and control forms. This is similar but less well defined than the ISA/IEC 62443 requirements for partitioning a System Under Consideration (SUC) into zones and conduits as well as the requirements for assessing the cyber security risk and determining the Security Level – Target (SL-T) for each defined zone and conduit.

83. The RP's CSAP is based on the principles of NEI 10-04 (ref. [83]), NUREG/CR-6847 (ref. [84]) and CSA N290.7:21 (ref. [85]) upon which they have devised a common definition of CEA to satisfy US and Canadian

Regulators. It was noted that NUREG/CR-6847 US Cyber Security Self-Assessment Method for Nuclear Power was dated Oct 2004.

84. Therefore, whilst the high-level process and intent of the CSAP risk assessment process is clear in its desire to identify CEAs, the process for identifying its susceptibility to cyber-attack is drawn from a 20 year old cyber self-assessment tool and the cyber security controls applied to mitigate those threats are drawn from US and Canadian standards. SyAPs recommends that reviews of security should be carried out to ensure arrangements remain up-to-date, including “comparisons with current modern standards”. It is my expectation that either modern, up-to-date standards are applied, or a gap analysis between older standards and current standards is undertaken to determine whether all relevant threats and risks are addressed.

85. I submitted Regulatory Query [RQ-01877], in which I requested the RP to clarify the rationale for selection of differing national cyber security assessment processes and control sets selected for the BWRX-300 CSAP and to clarify how the RP would intend to utilise the CSAP in a manner that would meet UK regulatory expectations highlighted above.

86. In its response (ref. [86]), the RP stated that the BWRX-300 System CSAP was adapted to the US NRC and CNSC regulatory requirements. It was decided to develop the CSAP using the methodology based on US NRC NUREG-CR6847 rather than IEC 62443 standard due to the CNSC CSA 290.7.21 explicitly referencing NUREG-CR6847 as an acceptable methodology, and that because the lead project was in Canada, this methodology was selected on that basis.

87. As a future development, the RP has stated it can adapt the CSAP to align with external, up-to-date international standards such as IEC 62443 or NIST SP 800-82 r3. The RP has committed to this in the Forward Action Plan (ref. [78]).

88. I considered this to be a proportionate and appropriate response, demonstrating appreciation of the matters raised in the RQ and a flexible approach to addressing a future development.

89. I judge that the RP’s CSAP meets expectations for Step 2 of GDA in that the methodology is fundamentally adequate for a generic cyber security assessment process, and is sufficiently flexible in design that it can be adapted to meet site-specific requirements, and is capable of demonstrating the relevant outcomes expected from a CPS.

4.3.3. Cyber Security Risk Analysis

90. My assessment plan articulated the intention that I would assess the RP’s methodology for identifying and mitigating cyber security risks and its application against a sample CBSIS so to evidence its efficacy against

SyAPs expectations. This includes consideration of the claims made on SbD for design of the CBSIS and that there is a strategy for future demonstration of production excellence for cyber security and independent cyber security assurance measures.

91. I would expect SbD to feature prominently in design documentation and processes in order to ensure security is considered in all relevant design decisions, with engineers and designers collectively seeking to reduce and eliminate security risk. I sampled the current iterations of the BWRX-300 Software Development Lifecycle (SDLC) and BWRX-300 Software Quality Assurance Program as a means to demonstrate SbD and identify or describe which specific aspects meet the requirements of SbD. These documents do make significant reference to SbD in the planning lifecycle, meeting my expectations for inclusion of SbD in project documentation and processes.

92. The RP applied its CSAP to three systems: the primary protection system (C10)(ref. [75]); the diverse protection system (C20)(ref. [76]); and the electrical power supply control system (C34) (ref. [77]). The RP produced and submitted CSARs for these systems in order to demonstrate the effectiveness of the methodology.

93. The CSARs of C10 and C20 document the identification, classification, and the application of cyber security controls of those systems' CEAs for the BWRX-300 during the preliminary (BL2) design phase currently being undertaken for the Darlington New Nuclear Project. This provides me with confidence that the methodology could be credibly applied to the BWRX-300 design presented in the SSSE.

94. The system CSAR of the C34 Electrical Power Supply Control System documents the identification, classification, and the application of cyber security controls CEAs for the BWRX-300 during the conceptual (BL1) design phase.

95. All CSARs submitted are due to be updated again later this year using the next revision of the CSAP, and against the next design phase. By producing the risk assessments, the RP demonstrated that its risk assessment methodology aligns to its CSAP (detailed above).

96. The RP submitted Figure 1. which outlines the RP's cyber security risk assessment methodology, referencing key documents.

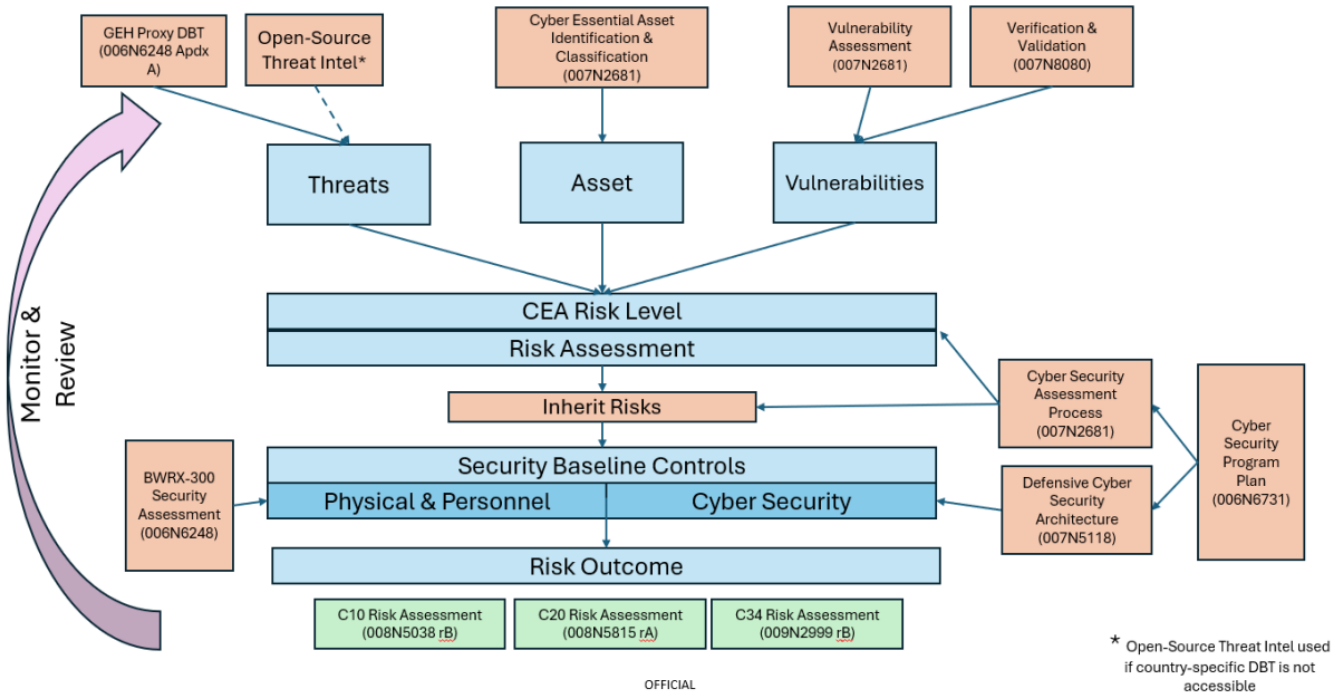

Figure 1. Outline of the RP's Cyber Security Risk Assessment Methodology

97. I noted that the RP had made the design decision to put in place a Diverse Protection System (DPS) based on a digital platform. The C&I inspector raised RQ-01743 to understand the types of digital technology proposed for use in the protection system in terms of maintaining adequate diversity and independence from the Primary Protection System.

98. I submitted a Regulatory Query [RQ-01903] in respect of the GVHA cyber security team's inclusion and consideration in the SbD evolution of the Safety Class 2 DPS to a digital platform, and how the security mitigations will maintain the fundamental design properties (including diversity and independence) of the Protection Systems both in its safety function and in the security design.

99. In response to the RQ (ref. [87]), the RP stated for the DPS, cyber security requirements for Safety Class 2 or moderate significance systems apply and are considered by the system designer during each design phase to ensure compliance where they are applicable, technically feasible, and do not adversely impact the system's functionality or performance.

100. The RP stated that the DPS was also risk assessed at an early design state to identify cyber security requirements after switching from analogue to digital. The RP claimed that this had led to a system that has been iterated using a SbD approach. It claimed that diversity is retained by using redundancy within the system and network design. A final formal risk

assessment of the DPS along with a justification for design choices is due during the next design phase as required by the DCSA.

101. The RP referenced the DCSA: “Verification and validation are key processes that confirm the cyber security requirements during the SDLC (Software Development Life Cycle) have been properly implemented, documented for requirement tracing, a risk assessment has been performed, and cyber security controls have been properly applied without negatively impacting CEA performance”.

102. I acknowledge that there is a cyclical process of validation and verification by an independent assessor. However, I judge that where there are related digital systems with fundamental design properties that include diversity and independence, the establishment and verification of these properties should be a documented part of the CSAP. In this case, there are claims of independence and diversity made in respect of the system’s relationship to each other. Yet, the cyber security aspects are examined in isolation, without consideration of the independence and diversity claims. The safety systems verification and validation process is not performed by cyber security specialists and, therefore, could compromise the diversity claims.

103. The C&I inspector has submitted a Regulatory Observation [RO-BWRX300-001] (ref. [88]) in respect of this matter, including the expectation that the RP considers how cyber security supports the principle of independence. The RP has produced a Resolution Plan [ref. [89]) which addresses this aspect, and I judge that the Resolution Plan and RP response are proportionate for Step 2 of GDA and will adequately address the matters raised in the RO in the future security case.

5. Conclusions

104. This report presents the Step 2 cyber security assessment for the GDA of the BWRX-300 design. The focus of my assessment in this step was towards the fundamental adequacy of the design and security 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. [11]) at the content of most relevance to cyber security against the expectations of ONR's SyAPs, TAGs and other guidance which ONR regards as relevant good practice.

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

- I judge that the RP's approach to cyber security risk management is fundamentally adequate for Step 2 GDA. Where deviations from modern relevant good practice were identified, the RP was proportionate and diligent in its response, with a willingness to address challenges to design and methodology which gave me confidence that the Forward Action Plans put in place would address site-specific expectations.

- The RP has indicated that it intends to use an all-digital I&C architecture. RO-BWRX300-01 has been raised by the C&I inspector to seek confidence that relevant safety and security expectations are met. The RP has committed to carry out further work, as defined in its Resolution Plan (ref. [89]), to substantiate its design decision, including consideration of how cyber security supports the principle of independence and how SbD principles are applied in this design decision making.

- The RP has developed its own 'proxy' DBT for the generic design, which is reasonable and contains generally accepted threats to inform and evaluate its CPS design. However, the UK DBT, together with UK URC thresholds will need to be taken into account in the future security case to ensure the required CPS outcomes is identified and met. The RP has acknowledged this and committed it to the Forward Action Plan.

- I am satisfied PSR Chapter 25 (ref. [3]) provides an adequate high-level overview of security and demonstrates an approach to cyber protection system design which is aligned with my regulatory expectations, including those defined in SyAPs.

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

References

[1] GE-Hitachi, NEDO-34162, 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-34197, BWRX-300 UK GDA Chapter 25 - Security, Rev B, 3 July 2025, ONRW-2019369590-22205.

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

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

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

[7] ONR, Security Assessment Principles for the Civil Nuclear Industry. 2022 Edition, Version 1, March 2022. ONR. www.onr.org.uk/syaps/security-assessment-principles.pdf.

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

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

[10] ONR, New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-006, Issue 1, August 2024. www.onr.org.uk/new-reactors/onr-gda-gd-006.pdf.

[11] ONR, Step 2 Security Assessment Plan for the Generic Design Assessment of the GE Hitachi BWRX-300, ONRW-2126615823-4730.

[12] ONR, BWRX-300 Step 2 Summary Report, Revision 1, December 2025, ONRW-2019369590-21328.

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

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

[15] 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[36] 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.

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

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

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

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

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

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

[43] 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.

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

[45] 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.

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

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

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

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

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

[51] GE-Hitachi, 007N5118, BWRX-300 Defensive Cyber Security Architecture, Rev A, 25 October 2024.

[52] ONR, The Nuclear Industries Security Regulations 2003: Classification Policy for the Civil Nuclear Industry, ONR-CNSS-POL-001, October 2004.

[53] HMG, Anti-Terrorism, Crime and Security Act 2001, www.legislation.gov.uk/ukpga/2001/24/section/79.

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

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

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

[57] 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.

[58] ONR, CNS-TAST-GD-11.4.1 – Secure by Design.

[59] ONR, Guidance on the Security Assessment of Generic New Nuclear Reactor Designs.

[60] ONR, CNS-TAST-GD-7.1 - Effective Cyber and Information Risk Management.

[61] ONR, CNS-TAST-GD-7.3 - Protection of Nuclear Technology and Operations.

[62] ISA, ISA/IEC 62443 – Security for Industrial Automation and Control Systems.

[63] National Institute for Standards and Technology, NIST 800 – 82 rev3 – Guide to Operational Technology Security.

[64] International Organization for Standardization, ISO 27001:2022 – Information Security Management Systems.

[65] GE-Hitachi, 006N5064, GE Hitachi Safety Strategy, Revision 6, March 2024, 2024/10561.

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

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

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

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

[70] GE-Hitachi, 006N6248, BWRX-300 Security Assessment, Rev 2, 15 July 2025, ONRW-2019369590-22483.

[71] GE-Hitachi, 007N2681, BWRX-300 System Cyber Security Assessment Process, Rev B, 25 October 2024.

[72] GE-Hitachi, 007N5118, BWRX-300 Defensive Cyber Security Architecture, Rev A, 25 October 2024.

[73] GE-Hitachi, 006N6731, BWRX-300 Plant Cyber Security Program Plan, Rev 2.

[74] GE-Hitachi, 007N8080, Cyber Security Controls for the Software Development Lifecycle, Rev A, 25 October 2024.

[75] GE-Hitachi, 008N5038, C10 BWRX-300 Primary Protection System Cyber Security Assessment Report, Rev B.

[76] GE-Hitachi, 008N5815, C20 Diverse Protection System Cyber Security Assessment Report, Rev A.

[77] GE-Hitachi, 009N2999, C34 Electrical Power Supply Control System Cyber Security Assessment Report, Rev B.

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

[79] GE-Hitachi, 007N0624, BWRX-300 Plant Instrumentation and Control Digital Systems and Software Process Engineering Software QA Program Plan, Rev 0.

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

[81] 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/.

[82] National Institute of Standards and Technology, NIST SP 800-82 Rev. 2 - Guide to Industrial Control (ICS) Security.

[83] US NRC, NEI 10-04 - Identifying Systems and Assets Subject to the Cyber Security Rule.

[84] US NRC, Cyber Security Self-Assessment Method for US Nuclear Power Plants.

[85] CSA, N290.7:21 - Cyber Security for Nuclear Facilities.

[86] GE-Hitachi, M250125, Submission of BWRX-300 UK GDA Step 2 RQ-01877 Response, 29 April 2025.

[87] GE-Hitachi, M250144, Response to RQ-01903, 29 April 2025.

[88] ONR, RO-BWRX300-001 Demonstration of independence and diversity in the BWRX-300 I&C Architecture, Rev 1, 20 June 2025, ONWR-21266115823-7689.

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

Appendix 1 – Relevant SyAPs considered during the assessment

SyAP reference	SyAP title
SyDP 7.1	Effective Cyber and Information Risk Management
SyDP 7.3	Protection of Nuclear Technology and Operations
KSyPP 1	Secure by Design
KSyPP 2	The Threat
KSyPP 3	The Graded Approach
KSyPP 4	Defence-in-Depth
Annex H	Cyber Protection System Outcomes