Office for Nuclear Regulation

ONR Assessment Report

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

ONR Assessment Report

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

Report Title: Step 2 Assessment of Protective Security

Authored by: Principal Inspector, Nuclear Security, ONR

Assessment report reference: AR-01615

Project report reference: PR-01880

Report issue: 1

Published: December 2025

Document ID: ONRW-2126615823-8070

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 protective 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 protective 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 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 because I consider they would enable me to decide on the fundamental adequacy of the design from a protective security perspective in terms of processes, methodologies, and approaches. I consider this particularly relevant because the physical protection system (PPS) is based on a generic design, informed by the RP's proxy Design Basis Threat (DBT) and not the UK DBT, which was unavailable to the RP in Step 2, and which the PPS will ultimately be designed to mitigate.

- The RP's methodology and approach to secure-by-design (SbD);
- The RP's approach to demonstrating defence-in-depth for security;
- The RP's approach to developing fundamental security functions of detect, delay, assess, control of access and insider mitigation; and
- The RP's application of its proxy DBT and approach to vulnerability assessment.

Based on my assessment, I have concluded:

- SSSE Chapter 25 - Security provides a good high-level overview of security and demonstrates an approach to physical protection system design which is aligned with my expectations;

- The RP has developed its own DBT for the generic design, which is reasonable and contains generally accepted threats to inform and evaluate its PPS design. However, a future SSSE will need to demonstrate use of the UK DBT, together with the application of UK unacceptable radiological consequence (URC) thresholds to undertake its Vital Area identification and determine the required PPS outcome. The RP has acknowledged this and committed it to the forward action plan;

- More detailed evaluation of the PPS will need to be undertaken to ensure that it can mitigate the threats documented in the latest UK DBT;

- The security architecture is consistent with the overall aim of providing defence in depth against the threats identified in the RP’s proxy DBT and, at a high level, aligns with RGP as set out in the ONR SyAPs annexes for the provision of security functions for detect, delay, assess, access control and insider mitigation; and

- The categorisation for sabotage of the design’s main inventory of nuclear material (NM) and other radioactive material (ORM) has been undertaken satisfactorily using the IAEA categorisation tables. However, future categorisation for theft will need to be completed using the tables in the SyAPs Annexes and include all NM and ORM inventory. The RP has acknowledged this and committed it to the forward action plan.

Overall, based on my assessment to date, I have not identified any fundamental 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 the application of the UK DBT and further assessment (in either a future Step 3 GDA or during site specific activities) of suitable and sufficient supporting evidence that can substantiate the claims and proposals made in the GDA Step 2 submissions.

List of abbreviations

ALARP	As Low as Reasonably Practicable
ABWR	Advanced Boiling Water Reactor
BTC	Basic Technical Characteristics
BWR	Boiling Water Reactor
CAE	Claim, Argument and Evidence
CAS	Central Alarm Station
CNC	Civil Nuclear Constabulary
CNS	Civil Nuclear Security
CNSC	Canadian Nuclear Safety Commission
CCTV	Closed Circuit Television
CS&IA	Cyber Security & Information Assurance
DAC	Design Acceptance Confirmation
DBT	Design Basis Threat
DEC	Design Extension Conditions
DESNZ	Department of Energy Security and Net Zero
DR	Design Reference
DRP	Design Reference Point
DRR	Design Reference Report
ESBWR	Economic Simplified Boiling Water Reactor
FAP	Forward Action Plan
FSyP	Fundamental Security Principal
GB	Great Britain
GDA	Generic Design Assessment
GVHA	GE Vernova Hitachi Nuclear Energy Americas LLC
GSE	Generic Site Envelope
GSR	Generic Security Report
HVM	Hostile Vehicle Mitigation
IAEA	International Atomic Energy Agency
IDS	Intruder Detection System
ICS	Isolation Condenser System
KSyPP	Key Security Plan Principle
LOCA	Loss of Coolant Accident
LTR	Licensing Topical Report
MCR	Main Control Room
MDSL	Master Document Submission List
NISR	Nuclear Industries Security Regulations (2003)
NM	Nuclear Material
NPP	Nuclear Power Plant
NPSA	National Protective Security Authority
NRC	Nuclear Regulatory Commission
NRW	Natural Resources Wales
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
ORM	Other Radioactive Material
PA	Protected Area

PAAB	Protected Area Access Building
PCSR	Pre-construction Safety Report
PID	Project Initiation Document
PIDS	Perimeter Intruder Detection System
PPS	Physical Protection System
PSA	Probabilistic Safety Assessment
PSAR	Preliminary Safety Analysis Report
PSR	Preliminary Safety Report
RGP	Relevant Good Practice
RITE	Risk Informed Targeted Engagement
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party
RQ	Regulatory Query
SAP	Safety Assessment Principle(s)
SAS	Secondary Alarm Station
SbD	Secure by Design
SFAIRP	So far as is reasonably practicable
SGI	(US) Safeguarded Information
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
SyAPs	Security Assessment Principles
SySSC	Security Structure, System and Component
SyDP	Security Delivery Principle
TAG	Technical Assessment Guide(s) (ONR)
TSC	Technical Support Contractor
UK	United Kingdom
UPS	Uninterruptible Power Supply
URC	Unacceptable Radiological Consequence
US	United States of America
VA	Vital Area
VAI	Vital Area Identification
WENRA	Western European Nuclear Regulators' Association

Contents

1. Introduction

1. This report presents the outcome of my protective 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 2, 3 and 25 (refs. [2], [3], [4]), the associated revision of the Design Reference Report (DRR) (ref. [5]) and supporting documentation.

2. Assessment was undertaken in accordance with the requirements of the ONR Management System and follows ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [6]) and ONR's risk informed, targeted engagements (RITE) guidance (ref. [7]). The ONR Security Assessment Principles (SyAPs) (ref. [8]), together with supporting Technical Assessment Guides (TAGs) (ref. [9]), 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. [10]).

1.1. Background

4. The ONR's GDA process (ref. [11]) 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.

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 currently 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. [12]). 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. [13]) and published on the regulators' website.

1.2. Scope

14. The assessment documented in this report is based upon the SSSE for the BWRX-300 (refs. [1], [2], [3], [14], [15], [16], [17], [18], [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], [4], [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 Design Reference Report (DRR) (ref. [5]) 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 Nuclear Power Plant (NPP) that is proposed for consideration in the GDA. The DRR provides a list of the systems, structures and components (SSCs) which are included in the scope of the GDA, and their relevant GDA reference design documents.

16. The RP has stated it has no 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 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 [6] and ONR's guidance on Risk Informed, Targeted Engagements [7].

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 DBT has been applied, the relevant PPS Outcome has been confirmed and site specific characteristics taken into account; and
- Instructions and concept of operations for security staff and response forces. These will be developed by a licensee in conjunction with relevant bodies such as the Civil Nuclear Constabulary and local police forces and determined by the security outcome once Vital Area Identification (VAI) has been completed using the UK Design Basis Threat (DBT).

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 security;
- The RP's approach to developing fundamental security functions of detect, delay, assess, control of access and insider mitigation;
- The RP's application of its proxy DBT and approach to vulnerability assessment; 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.

1.2.1. Protection of Sensitive Nuclear Information

21. This report contains sensitive nuclear information (SNI) relating to the assessment of the RP's PPS design which is US Safeguarded Information (SGI). This has been appended to allow for the main body of the report to remain as "OFFICIAL" information and releasable to the public. A limited amount of SNI[1] has been included in Appendix 2 to provide for a meaningful record of the assessment. This information has been categorised in line with the Classification Policy for the Civil Nuclear Industry (ref. [51]. In accordance with Section 79 of the Anti-terrorism, Crime and Security Act (ref. [52]), 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 SyAPs (ref. [8]) constitute the regulatory principles against which the RP's security 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. [53]) and Nuclear Security Series (ref. [54]) 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. [55]), which represent good practices for existing NPPs, and Safety Objectives for new reactors (ref. [56]).

[1] As defined in Section 77(7) of the Anti-terrorism, Crime and Security Act 2001

27. The relevant SyAPs and IAEA standards are embodied and expanded on in the TAGs (ref. [9]). The TAGs provide the principal means for assessing protective 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. Fundamental Security Principle (FSyP) 6 – Physical Protection Systems (PPS) has formed the basis of my assessment to ensure that the RP has implemented a proportionate PPS that builds defence-in-depth and is graded according to the potential consequence of a successful attack. To provide a judgement on fundamental adequacy of the RP's PPS, I have drawn upon the following supporting Security Delivery Principles (SyDPs) and Key Security Plan Principles (KSyPPs):

- SyDP 6.1 - Categorisation for Theft. Characterisation of the design according to quantities and form of Nuclear Material (NM) and Other Radiological Material (ORM) held or used is essential to determine the required PPS Outcome.

- SyDP 6.3 - Physical Protection System Design. A PPS should include functions such as deterrence, delay, detection, response and insider threat that is designed to meet the required outcome.

- SyDP 6.4 – Vulnerability Assessments. The RP should validate the efficacy of the PPS design through the conduct of vulnerability assessment to ensure it meets the required security outcome.

- KSyPP 1 – Secure by Design. The RP should apply security controls to reduce vulnerabilities during the design stage.

- KSyPP 2 – The Threat. The PPS should be designed and evaluated using a DBT which is likely to reduce the need for design changes when the UK DBT is applied in future stages.

- KSyPP 3 – The Graded Approach. The RP should design security systems using a graded approach where the most robust systems are designed to protect those areas that could give rise to the highest consequence in terms of theft of NM or ORM or the sabotage of NM or ORM and the systems protecting them.

- KSyPP 4 – Defence-in-Depth. The PPS should be designed to provide several layers of protection and methods of protection.

30. It should be noted that the PPS should be designed and implemented to build defence-in-depth and to meet the required security outcome based on

the categorisation for theft and sabotage. Ultimately, the categorisation for sabotage will be based on the application of the UK DBT (ref. [57]) and UK thresholds for unacceptable radiological consequence (URC) (ref. [58]) at the site perimeter; this will identify the appropriate PPS outcome that must be achieved. As these specific factors were unavailable to the RP and it could not therefore determine the required PPS outcome, I have based my assessment on sabotage categorisation for existing UK nuclear power plants (PPS Outcome 1), requiring the most robust PPS design.

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

2.1.2. Technical Assessment Guides (TAGs)

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

- NS-TAST-GD-096 - Guidance on Mechanics of Assessment (ref. [59])
- CNS-TAST-GD-11.1 – Guidance of the Security Assessment of Generic New Nuclear Reactor Designs (ref. [60])
- CNS-TAST-GD-6.1 - Categorisation for Theft (ref. [61])
- CNS-TAST-GD-6.2 – Physical Protection System Design (ref. [62]
- CNS-TAST-GD-6.4 - Vulnerability Assessments (ref. [63])
- CNS-TAST-GD-11.4.1 – Secure by Design (ref. [64])

2.1.3. National and international standards and guidance

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

- IAEA NSS 13 - Physical Protection of Nuclear Material and Nuclear Facilities (ref. [65])
- IAEA NSS 40T - Handbook on the Design of Physical Security Protection Systems for Nuclear Material and Facilities (ref. [66])
- IAEA NSS 8G – Insider Threats (ref. [67])

2.2. Integration with other assessment topics

34. 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 to ensure proportionate security arrangements have been adopted to protect those areas. I have worked closely with the STAR inspector and drawn upon the STAR assessment report (ref. [68]) to ensure appropriate SSCs and vital areas (VAs) have been identified and to determine the adequacy of the RP's SbD approach.

- **Cyber Security & Information Assurance (CS&IA)**. I have worked closely with the CS&IA assessor to ensure that those areas containing critical control and instrumentation (C&I) systems have appropriate physical protection in place.

- **Life Fire Safety (LFS)** I have engaged with the LFS inspector to ensure that the design of the PPS, particularly access control systems, do not compromise safety arrangements for emergency evacuation or access requirements for emergency responders.

2.3. Use of technical support contractors

35. I have not engaged Technical Support Contractors (TSCs) to support my assessment of the protective security 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 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.

38. This section presents a summary of the RP's protective 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.

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 widely used globally (ref. [15]).

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. Of particular relevance to security, is the RP's claim that all critical safety SSCs are located within the reactor building. The reactor is located within the power block, which itself is located within a protected area (PA), which the RP has included in its security case argument.

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 [69], [70], [71], [72]). 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 and secure, and that 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. [73]), supplemented to include UK specific chapters such as Structural Integrity and Chemistry. The RP has also provided a chapter on As Low as Reasonably Practicable (ALARP), which is applicable to all safety chapters. The RP has stated that the design and analysis referenced in the PSR is consistent with the March 2024 Preliminary Safety Analysis Report (PSAR) submitted to the US Nuclear Regulatory Commission (NRC). The Security Assessment and PER are for

the same March 2024 design but have more limited links to any US or Canadian submissions.

3.3. Summary of the RP's Case for 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 robust 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. Categorisation for Theft and Sabotage

48. The RP has undertaken analysis of areas containing NM or ORM, which it has determined to be important to plant nuclear safety and/or safety SSCs or prevention of a radiological release that, if sabotaged would be capable of causing a URC. It has designated these areas as Vital Areas (VAs) along with those areas whose loss would significantly impact the security response to a threat. The RP has also undertaken an exercise to determine the categorisation for theft. This has been undertaken based on a sample of four fresh fuel bundles at between 3.8% - 4.0% of U235. The RP has also included analysis of irradiated fuel. All analysis has been undertaken against IAEA tables (ref. [65]).

3.3.2. Protective Security

49. Protective security is provided through a combination of organisational capabilities including guards and response strategies; physical barriers such as walls, doors and fences; access controls, detection and surveillance systems; and adopting SbD and defence-in-depth philosophies. The RP has deployed these in a manner to protect identified VAs and its NM and ORM inventories and security sensitive areas.

3.3.3. Design Basis Threat

50. The RP has developed a 'proxy' DBT for its generic design that it considers establishes a set of credible characteristics, capabilities and techniques for the theft and/or sabotage of NM or ORM, providing assurance that a country specific DBT is capable of being successfully applied to the standard design without significant changes during subsequent country specific licensing. This is documented at Appendix A of the RP's security assessment.

3.3.4. Vulnerability Analysis

51. The RP has undertaken vulnerability analysis to satisfy itself that its PPS is effective and achieves proportionate protection to mitigate those threats documented in its proxy DBT. The analysis is documented at Appendix C of the RP's security assessment which details adversarial scenarios and those security arrangements in place to mitigate the effects of an attack. This is also supported by blast and breaching analysis and defensive strategies (Appendices F and H of the RP's security assessment).

3.3.5. Defence in Depth

52. The RP has documented its security arrangements to ensure there is a PPS design based on layers of defence designed to detect and delay adversaries in order that a response force can neutralise the threat. The layers of defence primarily relate to the Protected Area (PA) perimeter and Reactor Building, with a security infrastructure to monitor and assess alarms, to support a response.

3.3.6. Secure by Design

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

3.4. Basis of assessment: RP's documentation

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

- Chapter 25 (ref. [4]) – Security Annex of the PSR which outlines the overarching security case and is not protectively marked.

- The RP's Security Assessment Document and associated Annexes (ref. [74]) consisting 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, and HF engineering for security and software tools. It defines a proxy DBT encompassing threats that need to be mitigated, the identification of SSCs and areas requiring protection (such as VAs), the physical and cyber protection systems in place to mitigate threats and the evaluation of the effectiveness of these measures.

- The Forward Action Plan (FAP) (ref. [75]), which captures the commitments required to progress to GDA Step 3 or to a site specific phase.

55. The Security Assessment (ref. [74]) contains appendices which provide more detailed information to support the RP's security case:

- 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 - PPS Design Requirements
- Appendix O - Cross-reference to Requirements

3.5. Design Maturity

56. My assessment is based on Revision 3 of the DRR (ref. [5]). 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.

57. The reactor building 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 PA access building.

58. 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).

59. 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.

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

61. The PPS design has been developed to provide defence in depth to those significant safety SSCs that have been identified as part of the VAI process and require protection. However, it is important to note that the PPS has been developed to mitigate threats documented within the RP's own proxy DBT. The UK DBT will need to be applied to any VAI and vulnerability analysis processes to ensure that the appropriate security outcome can be identified and met.

4. ONR assessment

4.1. Assessment strategy

62. 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 protective 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 [76].

63. GVHA is currently engaging with regulators internationally, including the Nuclear Regulatory Commission in the US (US NRC) and the Canadian Nuclear Safety Commission (CNSC) in Canada. It is proposing a standard BWRX-300 design for global deployment with minimal design variations from country to country.

64. The UK's regulatory framework is outcome focused, with the PPS designed to build defence-in-depth to meet the required security outcome based on the categorisation for theft and sabotage. Two of the key factors in determining the categorisation for sabotage and hence the potential VA status of the design is the use of the UK DBT and the UK's definition of a URC. The UK DBT was not available to the RP during Step 2 and URC calculations are based on the RP's public access exclusion zone perimeter.

These details underpin the categorisation for sabotage and therefore the identification of the security outcome, and subsequent PPS design. For this assessment, I have focussed on the RP's methodologies for implementing an effective PPS for those areas it has identified as needing protection. In lieu of defined security outcomes, I have made judgements conservatively using the SyAPs Annexes C – D. Having considered discussions with the RP and the information documented in the security case relating to VAs and armed response, and outcomes required for existing UK NPPs, I have chosen to use PPS Outcome 1 – the most stringent of security outcomes in forming my judgement.

65. 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 PPS. Where necessary, I have sought clarification through the issue of regulatory queries (RQs).

4.2. Assessment Scope

66. 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.

67. 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.

68. 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 protective 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.

69. To fulfil the aims for the Step 2 assessment of the BWRX-300, I have assessed the following items, which I consider important:

- **Categorisation for Theft and Sabotage**. I assessed whether the RP has adequate methodologies in place for categorisation for theft and, drawing on the STAR assessment report (ref. [68]), has adequately categorised the plant for sabotage;

- **Design Basis Threat**. I assessed how the RP has used a DBT to design, evaluate and test its PPS. In lieu of access to the UK DBT, I have assessed whether the attributes of the RP's proxy DBT generally meet widely accepted expectations and how the RP will use the UK DBT in a future step or licensing;

- **Secure by Design.** 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 security measures. I also sought confidence that the process is repeatable for any UK specific security requirements, for example, post UK DBT application; and

- **Physical Protection System Design**. I assessed the RP's arrangements for delivering a protective security regime that sits within the wider plant risk management system and encompasses the functions of detect, assess, delay, access control and insider mitigation.

4.3. Assessment

4.3.1. Categorisation for Theft

70. To determine proportionate physical protection measures against unauthorised removal of NM and ORM, and in line with SyDP 6.1, dutyholders should undertake a characterisation of their facilities to determine the categorisation for theft. The RP has used the IAEA table, Categorisation of Nuclear Material (IAEA NSS No.13) (ref. [77]) to categorise the material within its facility. The SyAPs Annex A, tables and NISR 2003 Schedule 1 reflect the IAEA categorisation, and I am satisfied that the security case adequately categorises the proposed fuel in the reactor design for GDA Step 2. The RP's categorisation has been limited to the Reactor Building with the RP acknowledging there is further categorisation to be undertaken, using SyAPs and taking into account the radwaste building which is still under development. In addition, I noted the level of enrichment of fuel to be used in the reactor is similar to that used in existing operating reactors in the UK. The information that has been submitted is consistent with my expectations, as set out in relevant good practice/IAEA standards.

71. I have taken into account the RP's commitment in the FAP to use the categorisation values contained in SyAPs Annex A tables and consider all future NM and ORM inventories in its calculations. I am content that there are no fundamental shortfalls in the RP's methodology for categorisation for theft which would prevent the RP from further developing the generic BWRX-300 design and associated SSSE evidence to support any future permissioning activities for the construction of a power station based on the design.

4.3.2. The Physical Protection System Design

72. My expectation for Step 2, as documented in my assessment plan was for the RP to be able to demonstrate that it had applied key principles of SbD, defence in depth and had documented this in the security case, identifying how the key security functions of delay, detect, assess, and access controls and insider mitigation were applied to the overall design. My overall aim was to ensure that these principles were understood and applied at a high-level and that the RP had considered relevant aspects of modularisation, the compact nature of the design and likely smaller site footprint.

73. The overall level of detail in the BWRX-300 Security Assessment met my expectations for Step 2. Some of the response strategies and optioneering were out of scope of my assessment. However, I was encouraged to see that scenarios were being adopted, and adversarial pathway modelling was being used effectively to evaluate the PPS. A limitation of the PPS presented by the RP is that it is based on a proxy DBT in lieu of access to the UK DBT in Step 2. However, I consider that the assumptions made in the RP's DBT generally align with both national and international expectations (IAEA NSS 10G and CNS-TAST-GD-11.4.2) in that it relates to aspects of both insider and external adversaries and both physical and cyber threats.

74. Detailed information related to the PPS and my judgement on these arrangements are detailed in the SNI Appendix 3 to this report. However, my high-level observations and judgement are set out below.

4.3.2.1. Design Basis Threat

75. 'The Threat' is one of ONR's KSyPPs, which is fundamental towards meeting security expectations and underpins KSyPP 1, Secure by Design and KySPP 3 – Graded Approach. IAEA guidance and ONR SyAPs reflect that it is essential that a PPS is designed, evaluated and tested using a DBT. The UK Government's DBT refers to the malicious capabilities required to underpin the VA identification process, to determine the required SyAPs security outcome.

76. The RP's ability to utilise the UK DBT has been problematic due to access and handling challenges of this sensitive document. The RP's UK contractor made efforts to gain access to the UK DBT; however, was unable to gain access before the end of Step 2.

77. The RP has used a proxy DBT to set out the capabilities of hostile actors, which it has used to aid the design of security measures to prevent the effects of a URC focussing on the sabotage of NM or ORM or facilities. Its intention is to use this proxy DBT in its standard design prior to using country specific DBTs later in the design stage beyond Step 2. Originally termed a 'bounding' DBT, the RP has been open to suggestions to use an alternative term as I considered that any assertion that a proxy DBT bounds a state DBT can only be made once it has gained access to the UK DBT and undertaken some form of gap analysis/comparison. The RP has updated PSR Chapter 25 and the Security Assessment Document to reflect its use of a 'proxy' DBT.

78. I have worked closely with the ONR STAR assessor, who requires a DBT be used in Vital Area identification (VAI). They raised an RQ (RQ-01929) to clarify the use of the UK DBT. The RP's response (ref. [78]) clarified the aims and use of the proxy DBT to create 'risk reduced and robustness assurances'.

79. The RP's PSR, Chapter 25 Revision 2, commits the RP to using the UK DBT beyond Step 2 of the GDA and will replace Appendix A of its Security Assessment Document with the UK DBT. I am satisfied that the RP has adequately committed this to its FAP (ref. [75]) as reflected in Annex B of the PSR Chapter 25.

80. I have reviewed the RPs proxy DBT, to understand its characteristics and, while I have not repeated the specific details in this report, I am satisfied that some of the high-level assumptions generally accepted as RGP (KSyPP 2), such as the recognition of the insider threat, external threats and cyber threats/blended attack, have been taken into account in the proxy DBT, which allows for a SbD principle to be applied at what I consider to be a satisfactory level for GDA Step 2. Additionally, I consider that the RP has used its DBT appropriately to develop a list of adversarial scenarios at Appendix K of its Security Assessment document for application to the PPS to evaluate its design and performance. If it applies similar methods using the UK DBT as part of a future UK project, it is my opinion that it should be possible to demonstrate an effective PPS that meets the required security outcome.

81. I am content that there are no fundamental shortfalls in the RP's protective security submission which would prevent the RP from further developing the generic BWRX-300 design and associated SSSE evidence to support any future permissioning activities for the construction of a power station.

4.3.2.2. Secure by Design

82. SbD is a KSyPP. For Step 2, my expectation was that the RP could demonstrate a sound understanding of SbD and have an effective methodology for applying it. I also examined the examples of SbD provided by the RP in its security case. My main effort was to assess how the RP integrated security within the design process and the impact this had on design. I found that within its VAI process, the RP's initial step was to identify critical functions to ensure the ability to:

- Shut down the reactor and maintain sub-criticality.
- Cool irradiated fuel in the core and spent fuel pool.
- Prevent or limit the release of radioactivity affecting the public.

83. Through discussions with the RP, I was able to determine how the Responsible Engineer (RE) for security interacted with RE's from other disciplines to develop the design and deconflict where necessary. The RP describes how the Chief Engineer's Office conducts and documents formal design reviews periodically and at the end of each stage of the design process (Conceptual Design, Preliminary Design and Detailed Design), and how security is integral to this process. In the SSSE Chapter 25 – Security,

the RP provided examples of areas of design enhancements which benefit security:

- Reduction in the number of entrances to the reactor building, whilst still satisfying emergency evacuation requirements;
- Movement of critical systems such as the isolation condenser system (ICS) pools and the spent fuel pool away from the external wall;
- Thickening of spent fuel walls with additional steel cladding on both sides of the walls;
- Reactor building wall construction using diaphragm plate-steel plate composite and its inherent benefit to mitigate the effects of blast;
- Redesign of the Isolation Condenser System (ICS) piping to be inaccessible by routing directly from containment to the ICS heat exchangers in the ICS cooling water pools to eliminate potential exposure to malevolent action;
- Upgrade of key doors and hatches to be substantially more robust against explosive breaching. Security accredited doors are designed to be equally robust as the walls in which they are located;
- Enhancement of large ducts and openings to maintain the same robustness to breaching as the walls in which they were located; and
- Movement of bulk deliveries and hazardous material to outside the PA to reduce the opportunity for the introduction of hidden explosive devices and or resources for malicious activity.

84. In discussion with the RP, it was evident that there was considerable recognition that there are aspects of the design that have intrinsic security benefits and some, such as upgrades to key doors and hatches are clearly driven by security requirements. In other areas, such as the location of the ICS cooling water pools and spent fuel pond, the RP was able to demonstrate that it had applied its DBT during security reviews to create a design requirement to mitigate certain threat vectors. I consider that the inherent value and benefits of these designs to security have been recognised and factored into the security design and vulnerability analysis, and the examples provided together with supporting analysis demonstrate how the security hierarchy of controls has been considered by the RP.

85. I consider it important that the RP has adequately demonstrated effective integration of security in the design process to provide confidence that the development of the design will capture GB specific requirements, such as the application UK DBT and that the RP can demonstrate an integrated security design. I raised a regulatory query (RQ-01916), for the RP to show the process it adopts to demonstrate SbD and integration. The RP’s

response (ref. [79]) provided an example of the security system interface with other disciplines such as power and life safety for the build of the Protected Area Access Building (PAAB) and PA fence. The RP further provided me with an adequate explanation of its process during a security meeting (ref. [80]).

86. I judge that the RP has adequately demonstrated that it adopts an effective SbD approach to developing its security arrangements which is consistent with KSyPP 1 – Secure by Design.

87. I am content that there are no fundamental shortfalls in the RP's protective security submission which would prevent the RP from further developing the generic BWRX-300 design and associated SSSE evidence to support any future permissioning activities for the construction of a power station.

4.3.2.3. Defence-in-Depth

88. The RP has identified key areas where its security architecture provides defence in depth, these are explained in more detail in Appendix 3:

- **PA Perimeter.** Where the RP has detailed the measures for delaying both adversarial 'on-foot' approaches and from hostile vehicles through a combination of fences and barriers, together with the deployment of detection and assessment technologies to support an appropriate response;

- **PAAB**. The main point of access into the PA, which facilitates the verification of identity and authorisation, controls access, undertakes searching and screening of personnel and baggage, and manages access arrangements for visitors;

- **Vehicle Access Points**. A main access point for the PA facilitating vehicle authorisations, searches and validating credentials. Use of a sally port arrangement facilitates access while maintaining a continuous barrier to the PA; and

- **Reactor Building**. Where further barriers, detection and access control arrangements are in place. This is a significant structure, the construction of which the RP has used to underpin significant resilience to threats.

89. I judge that the RP has adequately demonstrated that its PPS is configured in a way which provides defence in depth and that it has evaluated this against several scenarios albeit, based on its proxy DBT. I consider its approach is consistent with KSyPP 4 – defence-in-depth.

90. I have assessed the RP's arrangements and strategy for developing its PPS and found it to be mature for a generic design. I have assessed the PPS against RGP - the UK's National Protective Security Authority (NPSA)

guidance (ref. [81]) and IAEA NSS N0.40T, Handbook on the Design of Physical Protection Systems for Nuclear Material and Facilities (ref. [66]) and found the arrangements satisfactory, with good evidence of evaluation of the measures against a range of adversarial scenarios. In my opinion, given the compact nature and modular design, the RP has considered security requirements and has designed areas for computer-based systems important to security (CBSy), a central alarm station (CAS) and secondary alarm station (SAS) and identified the need for robust power distribution and back-up to support the security infrastructure. The information that has been submitted is consistent with my expectations, as set out in RGP found in NPSA and IAEA guidance.

91. I am content that there are no fundamental shortfalls in the RP's protective security submission which would prevent the RP from further developing the generic BWRX-300 design and associated SSSE evidence to support any future permissioning activities for the construction of a power station.

5. Conclusions

5.1. Conclusions

92. This report presents the Step 2 protective 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, Security Assessment and relevant supporting documentation provided by the RP to form my judgements. I targeted my assessment, in accordance with my assessment plan (ref. [12]), at the content of most relevance to protective security against the expectations of ONR's SyAPs, TAGs and other guidance which ONR regards as RGP, such as IAEA NSS 13 (ref. [65].

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

- PSR Chapter 25 provides a good high-level overview of security and demonstrates an approach to physical protection system design which is aligned with my expectations.
- 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 PPS design. However, the UK DBT, together with UK URC thresholds will need to be applied to the VAI and vulnerability analysis processes to ensure that the appropriate security outcome can be identified and met. The RP has acknowledged this and commited it to the FAP.
- Further evaluation of the PPS design will need to be undertaken in future GDA steps or licensing to ensure that the design can mitigate the threats documented in the latest UK DBT.
- The security architecture is consistent with the overall aim of providing defence in depth against the threats identified in the RP's proxy DBT and, at a high level, aligns with SyAPs and IAEA expectations for the provision of security functions for detect, delay, assess, access control and insider mitigation.
- The categorisation for sabotage of the design's main NM and ORM inventory has been undertaken satisfactorily using the IAEA categorisation tables. However, future categorisation for theft will need to be undertaken using the tables in the SyAPs Annexes. The RP has acknowledged this and commited it to the FAP.

94. 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 protective security shortfalls that could prevent ONR

permissioning the construction of a power station based on the generic BWRX-300 design.

References

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

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

[3] GE-Hitachi, NEDC-34164P Chapter 2 Site Characteristics, Rev A - 20 November 2024, ONRW-2019369590-14923.

[4] GE-Hitachi, NEDC-34197P BWRX-300 UK GDA Chapter 25 - Security, Rev A, 20 November 2024, ONRW-2019369590-14914.

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

[6] 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.

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

[8] 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.

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

[10] ONR, Guidance on the Production of Reports for Permissioning and Assessment, NS-TAST-GD-108, Issue No. 2, December 2023..

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

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

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

[14] GE-Hitachi, E-Hitachi, NEDO-34165, BWRX-300 UK GDA Chapter 3 - Safety Objectives and Design Rules for SSCs, Revision C, ,5 July 2025, ONRW-2019369590-22497.

[15] GE-Hitachi, NE-Hitachi, NEDC-34166P, BWRX-300 UK GDA Chapter 4 - Reactor (Fuel and Core), Revision C, 15 July 2025, ONRW-2019369590-22500. .

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

[17] GE-Hitachi, GE-Hitachi, GE-Hitachi, NEDO-34168, BWRX-300 UK GDA Chapter 6 - Engineered Safety Features, Revision B11 July 2025, ONRW-2019369590-22395., 11 July 2025, ONRW-2019369590-22395.

[18] GE-Hitachi, GE-Hitachi, NEDO-34169 BWRX-300 UK GDA Chapter 7 - Instrumentation and Control, Revision B, 15 July 2025, ONRW-2019369590-22414.

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

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

[21] GE-Hitachi, GE-Hitachi, NEDO-34172 BWRX-300 UK GDA Chapter 9B - Civil Structures, Revision B, 15 July 2025, ONRW-2019369590-22416.

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

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

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

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

[26] GE-Hitachi, GE-Hitachi, NEDO-34177 BWRX-300 UK GDA Chapter 14 - Plant Construction and Commissioning, Revision B, 5 July 2025, ONRW-2019369590-22503.

[27] GE-Hitachi, GE-Hitachi, NEDO-34178 BWRX-300 UK GDA Chapter 15 - Safety Analysis, Revision 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, NEDC-34180P BWRX-300 UK GDA Chapter 15.2 - Safety Analysis Identification Categorization and Grouping, Rev B, July 2025, ONRW-2019369590-22505.

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

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

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

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

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

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

[36] GE-Hitachi, GE-Hitachi, NEDO-34187 BWRX-300 UK GDA Chapter 15.9 - Safety Analysis - Summary of Results of the Safety Analyses, Revision B, 15 July 2025, ONRW-2019369590-2251.

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

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

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

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

[41] GE-Hitachi, NEDC-34192P Chapter 20 Environmental Aspects, Rev A, 20 November 2024, ONRW-2019369590-14932.

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

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

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

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

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

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

[48] GE-Hitachi, NEDC-34200P Chapter 28 Safeguards, Rev B, 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] ONR, The Nuclear Industries Security Regulations 2003: Classification policy for the civil nuclear industry, ONR-CNSS-POL-001, October 2024.

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

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

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

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

[56] 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.

[57] HMG, UK Design Basis Threat, 2003.

[58] ONR, ONR Security Assessment Principles for the Civil Nuclear Industry, 2022, Annex B Categorisation for Sabotage.

[59] ONR, NS-TAST-GD-096 - Guidance on Mechanics of Assessment.

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

[61] ONR, CNS-TAST-GD-6.1 - Categorisation for Theft.

[62] ONR, CNS-TAST-GD-6.2 – Physical Protection System Design.

[63] ONR, CNS-TAST-GD-6.4 - Vulnerability Assessments.

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

[65] IAEA, IAEA NSS 13 - Physical Protection of Nuclear Material and Nuclear Facilities.

[66] IAEA, IAEA NSS 40T - Handbook on the Design of Physical Security Protection Systems for Nuclear Material and Facilities.

[67] IAEA, IAEA NSS 8G – Insider Threats.

[68] ONR, ONR AR-01360, Sabotage, Target Analysis and Review Assessment Report, ONRW-2126615823-8075.

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

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

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

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

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

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

[75] NEDC-34274P, Revision 2, GE Hitachi BWRX-300 UK GDA Forward Action Plan, July 2015.

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

[77] IAEA, NSS No 13 - Nuclear Security Recommendations pn Physical Protection of Nuclear material and Nuclear Facilities.

[78] GE Hitachi, M250158 - Response to RQ-10929-Use of the UK DBT, 2025.

[79] GE Hitachi, M250156-Submission of BWRX-300 UK GDA GEH Response to RQ-01916 , ONRW-609516046-1715.

[80] ONR, GE Hitachi BWRX-300 CR-ONR-CR-25-008-L4 Security Design Meeting-April 25, ONRW-20193695590-19732.

[81] HMG, National Protective Security Authority - Building Protection.

Appendix 1 – Relevant SyAPs considered during the assessment

SyAP reference	SyAP title
SyDP 6.1	Categorisation for Theft
SyDP 6.3	Physical Protection System Design
SyDP 6.4	Vulnerability Assessments
KSyPP 1	Secure by Design
KSyPP 2	The Threat
KSyPP 3	The Graded Approach
KSyPP 4	Defence-in-Depth